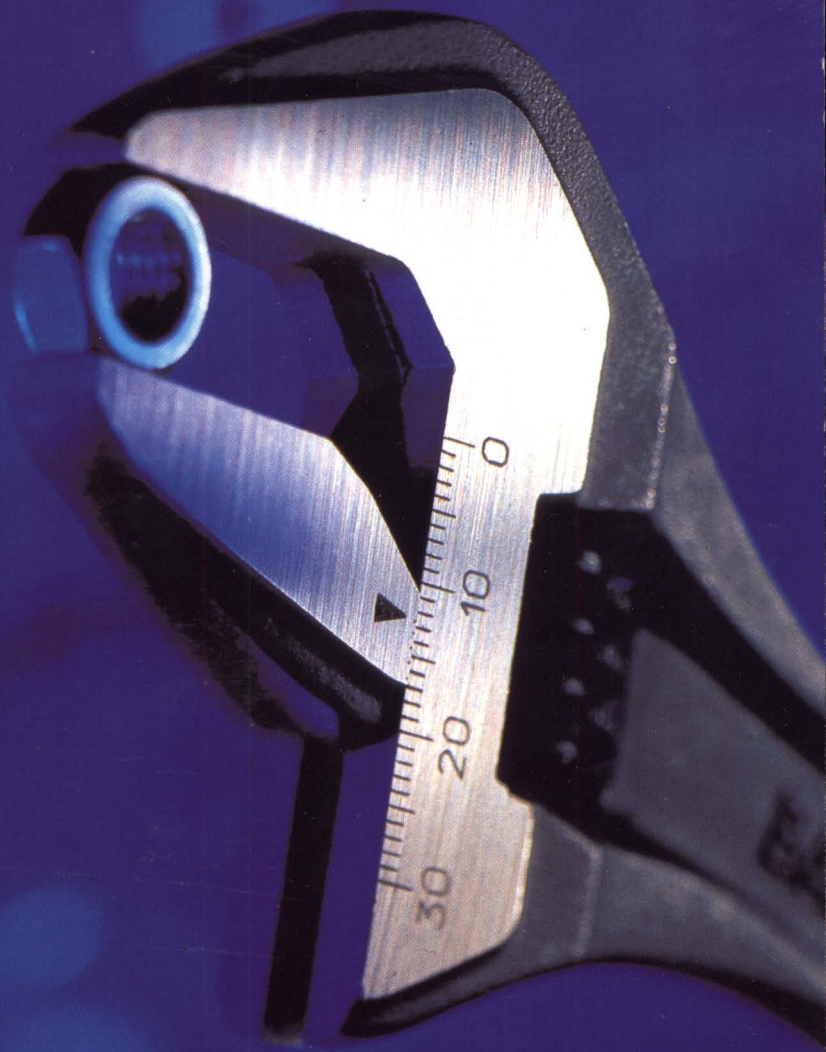
DR SOLOMON'S

Virus Encyclopedia



Dr Solomon's Virus Encyclopedia

Dr Solomon's Software Ltd.
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, UK
Tel: +44 (0)1296 318700 Fax: +44 (0)1296 318777
e-mail: support@uk.drsolomon.com

Dr Solomon's Software, Inc.
1 New England Executive Park, Burlington, MA 01803, USA
Tel: +1 617 273 7400 Fax: +1 617 273 7474
e-mail: support@us.drsolomon.com

Dr Solomon's Software GmbH
Luisenweg 40, 20537 Hamburg, Deutschland
Telefon: +49 (0)40 2519 54-0 Fax: +49 (0)40 2519 54-50
e-mail: support@de.drsolomon.com

CompuServe: GO DRSOLOMON
World Wide Web: http://www.drsolomon.com/

SS2101A-00-00-7.0

Copyright Dr Solomon's Software Ltd.

Dr Solomon's Anti-Virus Toolkit is copyright © 1993,1994, 1995, 1996 Dr Solomon's Software Ltd. All rights reserved. Dr Solomon's Anti-Virus Toolkit is not copy-protected. This does not mean that you can make unlimited copies of the disks. Dr Solomon's Anti-Virus Toolkit is protected by the copyright laws which pertain to computer software. It is illegal to make copies of the programs other than as may be licensed or for purposes of backup without written permission from Dr Solomon's Software Ltd. No part of the manual or other documentation accompanying Dr Solomon's Anti-Virus Toolkit may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language, in any form or by any means, without the prior written permission of Dr Solomon's Software Ltd.

Disclaimer

Neither Dr Solomon's Software Ltd. nor anyone else who has been involved in the creation, production or delivery of Dr Solomon's Anti-Virus Toolkit or this manual makes any warranties with respect to the contents of the software or this manual and each specifically disclaims any implied warranties to the extent allowed by legislation. Dr Solomon's Software Ltd. reserves the right to revise the software and the manual and to make changes from time to time in the contents without obligation to notify any person.

Trademarks

Dr Solomon's is a registered trademark of Dr Solomon's Software Ltd.. All other product names mentioned are acknowledged to be the trademarks of their producing companies.

Manual edition

5.0

October 1996

ISBN 1 897661 16 9 Dr Solomon's Virus Encyclopedia

Contents

Contents iii

Preface v

1. About Viruses 1

2. Virus Prevention 15

3. Networks and Viruses 19

4. A Brief History of Viruses 21

5. Mechanisms of Stealth 43

6. Polymorphic Viruses 49

7. PC Viruses 55

Glossary 365

Index 375

Preface

The Virus Encyclopedia gives background information about viruses and includes details of many of the viruses which the Anti-Virus Toolkit can detect. The Encyclopedia categorizes each virus, describes its effects and explains how it can be removed. It also lists any alternative names (aliases) by which the virus is known.

How to use this manual

This manual comprises seven chapters.

Chapter 1 - About Viruses explains what computer viruses are and the damage they can do.

Chapter 2 - Virus Prevention describes the resources available in the Anti-Virus Toolkit to detect and remove viruses.

Chapter 3 - Networks and Viruses provides a brief description of how to prevent viruses spreading across networks.

Chapter 4 - A Brief History of Viruses describes how viruses have evolved from 1986 to the present-day.

Chapter 5 - Mechanisms of Stealth describes how viruses use stealth to conceal themselves.

Chapter 6 - Polymorphic Viruses describes the principles polymorphic viruses use to try and evade detection by scanners.

Chapter 7 - PC Viruses provides descriptions of individual viruses and indicates methods of removal.

Copyright © Dr Solomon's Software

If you need help

You can contact Dr Solomon's by any of the following methods:

UK Office

By telephone:	+44 (0)1296 318700
By fax:	+44 (0)1296 318734
By e-mail:	support@uk.drsolomon.com
By bulletin board:	+44 (0)1296 318810
By post:	Dr Solomon's Software Ltd. Alton House Gatehouse Way Aylesbury Buckinghamshire HP19 3XU United Kingdom

US Office

By telephone:	+1 617 273 7400
By fax:	+1 617 273 7474
By e-mail:	support@us.drsolomon.com
By bulletin board:	+1 617 229 8804
By post:	Dr Solomon's Software, Inc. 1 New England Executive Park Burlington MA 01803 USA

German Office

By telephone:	+49 (0)40 2519 54-0
By fax:	+49 (0)40 2519 54-50
By e-mail:	support@de.drsolomon.com
By post:	Dr Solomon's Software GmbH Luisenweg 40 20537 Hamburg Deutschland

World Wide

CompuServe:	GO DRSOLOMON
World Wide Web:	http://www.drsolomon.com/

Copyright © Dr Solomon's Software

1. About Viruses

What is the first thing to do if you think you have a virus?

Do not panic. Indeed, do not do anything. Have a cup of tea or coffee – do not start bashing away at the keyboard before you have determined what you ought to do. Our experience shows that a lot of the 'damage done by viruses' is actually damage done by people doing things before they have made sure of what they ought to do, which is another way of saying panic. So, do not panic.

What is a virus?

A virus is a program that copies itself.

That is the definition of a virus. In retrospect, it is unfortunate that the word 'virus' was used – it makes the problem sound a lot worse than it is, and people get the plural wrong (the plural is not 'viri' or even 'virii', it is 'viruses). It might have been better to use the word 'weed'. But we're stuck with 'virus'.

A virus need do no more than replicate in order to be a virus – indeed, 95% of viruses do no more than that, plus some trivial extra like beeping the keyboard, or displaying a message. And conversely, if a program does something nasty that you were not expecting, that does not make it a virus, unless it replicates. Such a program is called a 'trojan', after the famous horse of Troy.

Why are viruses bad news?

If a virus does nothing but copy itself, why do people get so worked up when they have one? For example, ***Form*** virus beeps every time you press a key on your keyboard on the 18th of each month, so why does everyone who gets infected want to get rid of it? There are several reasons for this. If you run Windows 95 and you get a partition virus, then even if the virus does nothing, you'll lose 32 bit disk access, so your computer will run somewhat slower than it would have. Also, if you do not get rid of the virus, there is a strong likelihood that eventually you will pass it on to a supplier or customer, who will be upset.

Over 99% of viruses that actually spread in the wild are memory-resident. Therefore, there is the possibility of incompatibilities between the virus and other programs you run (for example, ***Jerusalem*** tries to use one of the resources that Novell uses, so you

Copyright © Dr Solomon's Software

cannot run both Novell and ***Jerusalem*** on the same system). Even though the virus has been analysed and documented, you might remain nervous that the virus does more than has been documented, or that you have a different version of the virus. In almost every case that Dr Solomon's have seen, people want to get rid of the virus (apart, sometimes, for keeping one specimen for a 'zoo').

Removing viruses takes time, and time is money. Each PC will take a minimum of several minutes, and each floppy disk will take a minimum of several seconds (and there may be a lot of floppy disks). It would be nice if you only had to worry about those PCs and floppy disks that are infected, but of course you do not know which ones these are until you have done the virus-hunt, so you have to check everything.

Things that are not viruses

Bugs

Bugs are not viruses, and viruses are not bugs. You may work with a large file for a long time. Eventually something goes wrong inside the program, and it refuses to let you save the file to the disk, so that you lose all the work you have done since the last save. The program might come from a major software house, but they would not make it go wrong on purpose, so it is not a trojan. The programmers made a mistake. Programmers are human, and humans make mistakes. Programmers, like other humans, have pride, and do not like to admit that they make mistakes, so they call them 'bugs', as if the bug had drifted in through the window and settled on the program. All sufficiently complex programs have bugs.

Anti-virus software does not detect bugs.

False alarms

False alarms are not viruses. A false alarm is when you think you have a virus, but you are mistaken. Sometimes, you have some hardware or software fault, and after running some diagnostics, you eliminate the possibility of hardware or software problems, conclude that it is therefore a virus, and proceed on that assumption. More often, a false alarm is the result of running anti-virus software.

Anti-virus software, in common with other software, is not infallible. The two main mistakes that an anti-virus program can make are to fail to find a virus that is there (once a program was tested that failed to find any boot sector viruses whatsoever,

 Copyright © Dr Solomon's Software

and these account for over two thirds of infections), or to claim that a virus is present when there is not. That is called a false alarm.

When an anti-virus program gives a false alarm, it looks pretty much like the real thing. However, there are certain things that might indicate that the alarm is false:

1. Only one file is giving the alarm (or perhaps four files, but they are copies of the same file).
2. Only one product gives the alarm – other products say the system is clean.
3. You get the alarm after running multiple products, but not when cold-booting and running any one product.
4. The virus that is detected is not listed as in the wild (of course, this list changes all the time).
5. The product says it cannot clean the virus.
6. The product says the virus is in memory, but when you boot clean, the product doesn't find a virus.

Unfortunately, there is no hard rule that can be applied. You cannot say it is a false alarm if one of the above six is true, or if all six of the above are true. The only way to really nail down a false alarm is to send the suspect file to the product vendor giving the alarm, and ask them to verify that it is a virus by analysing it in their virus lab. This could take up to 48 hours.

Meanwhile, a false alarm can be as much hassle as a real virus, or even more. A recent study (NCSA, 1996) said that a false alarm cost more that $20,000, which is somewhat more than most estimates of the cost of a virus. If you have a floppy disk that is infected with ***Stoned*** virus, you can simply copy the data off the disk and destroy the infected floppy disk, or you can get rid of the virus with your anti-virus program, or demand a replacement disk. Whatever, the cost is just a few seconds. But if you get an update of your preferred anti-virus program, and it tells you that you have ***Stoned*** virus on one of the files on your file server, then resolving the situation will take longer. By the way, ***Stoned*** cannot infect files. However, someone may have written a file virus and has decided to call it ***Stoned*** (for example, there are two unrelated viruses, one called ***Parity*** and the other called ***Parity Boot***). So, you send the file to your product vendor for analysis and comment. Meanwhile, to be safe, you remove the file from the server (or possibly the product is barring access to that file). This might mean that some important system will not work any more, as it needed that file. It also means that you have to keep track of the response to the problem, report it through the usual security breach reporting channel, and so on. You might

Copyright © Dr Solomon's Software

try deleting the offending file and re-installing the software that is causing the false alarm, but when you have finished doing that you still get the false alarm.

It is not surprising that some people have changed their anti-virus software after too many false alarms.

Jokes

A joke is something that is funny. Of course, what one person finds funny is not the same as what another person finds funny – it depends on your sense of humour. A program that pretends to format your hard disk, and then reveals that it has not – is that funny? It depends on your sense of humour.

Some people love to play practical jokes. So on certain dates you must apply a little scepticism to alleged virus reports. Some anti-virus software detects jokes, telling you 'You have a joke called....'. The reason for this, is that some jokes are fairly widespread, and are known to cause concern, so the anti-virus is trying to calm things down, by saying 'Yes, I know about this, and it is harmless'.

Hoaxes

There are a number of common hoaxes, which are widely believed. The most common of these is Good Times. This hoax has been around for a couple of years, and usually takes the form of a warning not to read any e-mail with Good Times in the title (often, the person putting out the warning puts Good Times in the title, without realising the humour of the situation). People pass along the warning because they are trying to be helpful, not realising the damage that this does. Every now and then, there's a fresh spurt of Good Times warnings.

The main way to deal with this issue, is not to pass on warnings unless they have come from a serious source.

Trojans

A trojan is a program that does something more than you were expecting, and that extra function is damaging. This leads to a problem in detecting trojans. Suppose a program was written that could infallibly detect whether another program formatted the hard disk. Could it be said that this program is a trojan? Obviously not – if the other program was supposed to format the hard disk (like Format does, for example), then it is not a trojan. But if you were not expecting the format, then it is a trojan. The

 Copyright © Dr Solomon's Software

problem is to compare what the program does with your expectations. You cannot determine a user's expectations of a program.

So, some judgements have to be made. The Aids Information Disk is generally considered to be a trojan. Approximately 20,000 copies of this were mailed to users in 1989, purporting to be a program that teaches you about Aids. In fact, it was a trojan – after you re-boot your computer 90 times, it encrypts and hides all the filenames on your hard disk, and demands that you pay for your license to use it. Although the documentation that came with it told you that something bad was likely to happen, it is generally considered to be a trojan. Format is not a trojan.

As a rule, you do not see trojans very often – they do not copy themselves, and do not spread in the way that viruses do. Trojans are not a real threat, except in either of the following circumstances:

1. When they are widely disseminated, like the Aids Information Disk.
2. They are targeted at an organization, in which case it is an 'inside job', carried out by someone within the company.

Some anti-virus products detect a few trojans (for example, the Aids one), but most products do not detect trojans at all.

Corrupted programs

Some files are simply corrupted (perhaps by a hardware problem), and hang the computer when run. For some reason, these sometimes end up in virus collections, unless the collection is carefully maintained. If you look at the collections that can be found on most underground virus exchange sites, you'll find 20% or 30% garbage files.

Intended viruses

Some virus authors are less skilful than they would like to be, and write what is clearly intended to be a virus, but for some reason there is such a major bug that the virus does not work at all. However, they release these in the fond belief that no-one will ever test them (or perhaps they did not test them themselves). One typical mistake is to get confused about decimal versus hexadecimal, and so their source code presumably says 'int 21' for the DOS function interrupt, but it should have said 'int 21h' (which is 33 in decimal).

Copyright © Dr Solomon's Software

Droppers

A dropper is a program that is not a virus, nor is it infected with a virus, but when run it installs a virus into memory, on to the disk, or into a file. Droppers have been written sometimes as a convenient carrier for a virus, and sometimes as an act of sabotage. Some anti-virus programs try to detect droppers.

Germs

A germ is an instance of the virus in generation zero, and in such a form that the infection could not have happened naturally. This is the original file created by the virus author. It might be an instance of the virus without any host file – if you remove the virus, you are left with a zero-byte file.

Different kinds of virus

Boot sector viruses

One of the most common kinds of virus are boot sector viruses, for example, ***Form*** and ***Stoned***. These infect the boot sectors of floppy disks, and either the Master Boot Record (MBR), or partition sector or the DOS Boot Record (DBR), or DOS boot sector of hard disks. The following example shows how a boot sector virus spreads:

1. You have been sent a floppy disk with data on it (perhaps some word-processed files and a spreadsheet). This is part of a project that you are doing jointly with a colleague. What your colleague does not know is that their computer is infected with a boot sector virus, and therefore so is the disk that has been sent to you. You put the disk in drive A: and start using these files. So far, the virus has not done anything. But when you finish for the day, you switch off the computer and go home. The next day, you come in and switch on. The floppy disk is still in drive A. So the computer tries to boot up from there. It loads the first sector into memory and executes it (normally, this is a small Microsoft program to load DOS), or if it cannot find DOS on the disk, tells you: 'Not a system disk, please press any key to continue'. Everyone has seen this message numerous times. So you do as instructed.
2. However this disk is infected with a boot sector virus, so what was executed was not just the program by Microsoft, but the virus as well. The virus installs itself on

 Copyright © Dr Solomon's Software

the hard disk, replacing the MBR, and copying the original MBR to a location a little further down the disk.

3. When you start up from the hard disk, the MBR runs, but this is the virus. The virus goes memory-resident, capturing the disk read/write interrupt 13h, and then it loads the original MBR, and the boot-up process continues as normal. However, since the disk read/write interrupt is captured, every time you make any write or read access to drive A: (you think you are making a read, but the virus decides to write anyway), the floppy disk is examined, and if it is not already infected, the virus is installed on the boot sector. Thus, your computer is now infecting every disk put in drive A:, and sooner or later one of these will be sent to a colleague, and the cycle continues.

The detail of various boot sector viruses is different, but the principle is the same. They are carried by the boot sectors of infected disks, and only in that way (for example, a boot sector virus cannot spread across a network). Thus the only way to get infected is to try to boot from an infected disk, even if the boot fails.

Boot sector viruses infect PCs. They do not care what operating system is running, or what security software is installed, because at the time the boot sector virus installs itself the operating system or security program is not yet running. However, with some non-DOS operating systems, although the PC is infected the virus cannot copy itself on to subsequent disks and cannot spread. It can, however, still do damage, as was discovered by one surprised Unix user when ***Michelangelo*** went off on March 6th.

To most people, the fact that viruses can infect in this way comes as a big surprise, which partly accounts for boot sector viruses being so common.

Boot sector viruses mostly work under DOS, Windows 3.x and Windows 95, but not under Windows NT or OS/2 (including Warp).

Macro viruses

The second most common kind of virus is the macro virus. Microsoft Word has a very powerful macro language, and it is possible to write viruses in that. The first such virus was the Concept virus (see the description). This virus was first seen in June of 1995, and by August it was quite common. By the end of 1995, it was challenging the

Copyright © Dr Solomon's Software

older boot sector viruses for first place in the frequency table. There are several other macro viruses, but none currently as common as Concept (July 1996).

Word macro viruses need Microsoft Word 6 or above, running on Windows 3.x, Windows 95, Windows NT or Macintosh. They spread by people sending infected document files to each other, entirely innocently, either on floppy disk, or via the internal LAN (often attached to e-mails), or via an external email system (such as the Internet).

TSR file viruses

A less common kind of virus is the Terminate-and-Stay-Resident (TSR) file virus. As the name suggests, these infect files, usually, these are COM and EXE files. There are however some device driver viruses, some viruses that infect overlay files, and although over 99% of executable programs have the extension COM or EXE, some do not.

For a TSR virus to spread, someone has to run an infected program. The virus goes memory-resident, typically looking at each program run thereafter and infects it (if it is not already infected). Some viruses are called fast infectors, and they infect if you just open the file (for example, a backup might open every file on the drive) – ***Dark Avenger*** was the first fast infector. In the case of ***Green Caterpillar***, the infection trigger is anything that determines what files are present (for example, DIR). Other triggers have been used, but the commonest is to infect each program that you are about to run.

Non-TSR file viruses

It is much easier to write a non-TSR virus, and so many of the budding virus authors do so. But it is quite rare for such a virus to be encountered in the wild – less than 1% of reported outbreaks are a non-TSR virus. With such a virus, running an infected program runs the virus, which at that time looks for another file to infect, and infects it. ***Vienna*** is the most common non-TSR virus, and even that is only seen very rarely these days. ***Vienna*** was the first file virus in the wild, and is still reported occasionally. There are a lot of viruses based on ***Vienna***, because a disassembly (almost equivalent to source code) was published in a book in 1987.

Copyright © Dr Solomon's Software

Companion viruses

If you have a COM file and an EXE file with the same filename and you type that name, DOS runs the COM file in preference to the EXE file. Companion viruses use this fact – each EXE file that you have acquires a companion COM file with the same name. Then, when you try to run your EXE program, the COM program is actually run, and that is the virus. When the virus has finished doing what it wants to do (for example, creating another companion for another file), it runs the EXE program, so everything seems to work normally.

There have been a few successful companion viruses, but not many. The main advantage to the virus author is that because the EXE file does not change, some change-detection software might not realise that a virus is spreading.

Another type of companion virus is the 'path companion'. This sort of virus puts a program in a directory that is earlier in the DOS PATH than is the victim. When you run a program that is not in your current subdirectory, DOS searches for the program in various subdirectories, as specified by the PATH command in your AUTOEXEC.BAT file. Path companions are harder to write than ordinary companions, so there are not many of them.

Overwriting viruses

An overwriting virus simply overwrites each file it infects with itself, and the program no longer functions. Because this is so glaringly obvious, overwriting viruses are never successful in spreading.

Multipartite viruses

Some viruses, for example, ***Tequila***, infect multiple objects. When you run a ***Tequila***-infected EXE, ***Tequila*** installs itself on the MBR. When you boot up the computer, ***Tequila*** runs from the MBR, and goes memory-resident. While ***Tequila*** is memory-resident, it infects EXE files.

Other viruses, for example, some of the versions of ***Anticad***, infect COM, EXE and MBRs interchangeably. Some viruses infect COM, EXE, MBRs and device drivers. Multipartite viruses are the third most common kind of virus.

Copyright © Dr Solomon's Software

Miscellaneous objects of infection

There are some viruses that infect OBJ files. The ***Starship*** virus infects by creating a new DBR, leaving the old one intact, leaving the code on the MBR intact, and changing the pointer in the MBR so that the ***Starship*** DBR is executed before the original DBR. The ***DIR II*** virus infects file systems by changing the File Allocation Table (FAT) and directories so that files on the hard disk are all cross-linked to the virus.

Virus characteristics

Fast infection

As explained previously, a fast infector spreads rapidly within a computer by infecting everything that is accessed. A fast infector is not as bad as it sounds – it is just as easy to clean a computer with 1000 infected files as one with 10, provided you have an anti-virus program that does a good cleaning job. However, most anti-virus products check memory for viruses. This is because of the possibility of a fast infector in memory. If there is a fast infector in memory, and the product opens all your files, you end up with every file on the computer being infected. This doesn't matter as much as it might sound, if you follow up by cleaning all those files with a good cleaner.

Slow infection

The opposite of a fast infector is a slow infector. The idea here is that if the virus spreads slowly, you are less likely to notice it and kill it. There are various ways that a slow infector might work, but the classic slow infector works by only infecting those files that you had intended to change anyway. This means that if you are running a change detector as an anti-virus measure, the change detector will trigger each time there is an infection, but since you had intended the file to change anyway, you will tell it to accept the change.

Starship is an example of another method of using slow infection – it only infects files as you copy them from your hard disk. So, no file on the hard disk ever changes, and the change detector is satisfied. But when you copy a file to a floppy disk, the copy is infected, and when you take this to another computer protected by the change detector, the change detector warns you of the existence of the new file. You then

 Copyright © Dr Solomon's Software

reassure the change detector that you knew about the new file, the change detector is satisfied, and another system is infected.

Stealth

If a virus is memory-resident (as are over 99% of viruses in the wild), then it has hooked at least one of the interrupts. If it is a boot sector virus, then it has hooked the disk read/write interrupt 13h. If it is a stealth virus, and any program tries to read the boot sector, then the virus says 'Aha, someone wants to see the boot sector – I will just read the original boot sector from where I put it, and present that instead'. So the software sees nothing out of the ordinary. ***Brain***, vintage 1986, was the first virus to use this trick. File viruses can use a similar trick to disguise their presence, so that any software reading the file sees only the bytes that were there before the virus came along – ***Frodo*** is an example. It is much more common to see stealth in boot sector viruses than in file viruses, as it is much easier for the virus author to implement stealth in a boot sector virus.

Stealth is covered in more detail in Chapter 5, "Mechanisms of Stealth".

Polymorphism

The commonest kind of anti-virus program that people use is the scanner, looking for a repertoire of viruses. Therefore, for the virus author, this is the kind of product that he would most like to defeat. A polymorphic virus is one where if you take two instances of the virus, there are no bytes in common between them, so you cannot

Copyright © Dr Solomon's Software

write down a byte-sequence and go looking for that to detect the virus. You have to do something a lot more complex and difficult.

Polymorphic viruses are covered in more detail in Chapter 6, "Polymorphic Viruses".

Damage done by viruses

We can categorize the damage done by viruses into six groups, according to the severity of the damage. Some authorities postulate the possibility of a virus that actually does good, but no-one has yet demonstrated such a virus.

We define damage as the virus doing something that you rather it did not do, and we quantify damage by measuring how long it takes to put things back to the way they ought to be.

We do not include consequential damage in this categorization (damage done by yourself in a mistaken attempt to get rid of the virus). For example, it is remarkable how many people will format the hard disk to try to repair ***Stoned***. All this does is lose all your data – the virus is untouched, as it resides in the MBR, which is not touched by Format. In addition, we do not include damage done by obscure incompatibilities between the virus and the system. For example, if a computer that was originally set up under DOS v2 (but now running a later DOS) is infected by ***Stoned***, then a large number of files will be corrupted because the design of the virus had not anticipated this situation.

Trivial damage

This is done by a virus such as ***Form*** (one of the most common viruses). On the 18th of every month, each key that you press makes the speaker beep. All you need to do is to get rid of the virus. This will usually take seconds or minutes (per computer). We would include under this category, viruses that cause Windows to avoid using 32 bit disk access.

Minor damage

A good example of minor damage is the way that the ***Jerusalem*** virus deletes any program that you try to run after the virus has gone memory-resident on Friday the 13th. At worst, you will have to reinstall some programs, but repairing the damage is unlikely to take more than 30 minutes per computer.

 Copyright © Dr Solomon's Software

Moderate damage

Moderate damage is done when a virus formats the hard disk, scrambles the File Allocation Table (FAT), or overwrites the hard disk. The damage is moderate only because you know that it has happened. You can reinstall DOS and reload yesterday's backup, because you do a backup every day. So, you will lose on average half a day's work, plus maybe an hour doing the reinstall and restore. The most famous virus for moderate damage is ***Michelangelo***.

Major damage

Major damage is done when a virus affects your backups as well as your hard disk. For example, every 16th time that a ***Dark Avenger***-infected file is run it overwrites a random sector on the hard disk with '**`Eddie lives... somewhere in time`**'. This might have been going on for several weeks. You discover ***Dark Avenger***, get rid of the virus, and find '**`Eddie lives`**' at several places in several files. You restore yesterday's backup, and find '**`Eddie lives`**' in the backup files. You might have to go back a few weeks before you can find clean data files. Then, when you have restored a 6-week old backup, you will find that you do not actually have any way to redo the work you have lost, because you do not have your original documents.

Severe damage

Severe damage is done when a virus makes gradual, progressive changes (so that backups are also corrupted), but the changes are not obvious (for example, there is no '**`Eddie lives`**'). You end up simply not knowing whether your data is correct or changed.

Unlimited damage

Some viruses (for example, ***Cheeba***, ***Vacsina.44.login*** and ***GP1***) aim to get the system manager password and pass it to a third party. In the case of ***Cheeba***, for example, it creates a new user with maximum privilege, with a fixed user name and password. Unlimited damage can then be done by the third party person, who can log in to the system and do anything.

Copyright © Dr Solomon's Software

How viruses are spread

It seems to be a common belief that viruses are spread by games, by shareware, or by Bulletin Board Systems (BBSs). The truth is more complex. Remember how the most common sort of virus (a boot sector virus) works – a physical disk has to be involved, and there does not need to be any software on it. You cannot get a boot sector virus by using a BBS.

The most likely routes by which a virus gets into an organization are engineers, parents, or colleagues:

1. Hardware engineers use disks on a large number of computers. This increases their chances of picking up an infected disk and spreading a virus.
2. Parents have children, and if there is a PC at home, and the children are young teenagers, then they quite possibly swap software at school. The disks that they bring home might well be infected, and if the parent is taking disks to and from work, a virus could easily be taken into work.
3. A boot sector virus could be on a data disk obtained from a colleague.
4. The commonest way for a macro virus to enter a company, is as an attachment to an e-mail.

Other ways of getting a virus include:

1. In shrink-wrapped software – some of the largest companies have accidentally shipped a virus in shrink-wrapped software.
2. Together with purchased hardware – most hardware comes with disks containing utilities or drivers.
3. Sales persons running demonstrations could unwittingly install the virus they picked up from the last place they ran their demonstration.

Copyright © Dr Solomon's Software

2. Virus Prevention

What can be done about viruses? A number of solutions have been proposed in the past. A few of these will be examined.

Certainly legislation helps. It reduces the number of viruses written, as Christopher Pile (alias "The Black Baron", author of the *Smeg* viruses) discovered when he was sentenced to an 18-months prison sentence. But it cannot make an impact on the thousands of viruses that already exist, and it slows down only slightly the creation of new viruses. Active measures have to be taken to deal with the viruses themselves. It cannot be hoped that viruses will go away.

Users do not regard computer problems as their own. They regard them as the domain of the MIS department. Users are too busy doing their jobs to pay any attention to looking out for viruses. So user education cannot be relied on. It simply does not work.

Users can be given precise procedures to follow, to check all incoming software, and about how to acquire software. Procedures tell users how to obey the rules. For example, the procedure for checking disks should be written down in detail – '**`Put the floppy disk in the drive, and type...`**'. If you have a sheep-dip computer, put the procedure up on the wall near to it. However, after a while, users just ignore procedures. A user may see a virus once in ten years. Thus, after six months of applying the 'time-wasting' procedures, they learn that when you go through the procedures, you do not find any viruses. So the procedures fall into disuse.

Procedures can be backed up with some rules. A good set of rules might be as follows:

1. Any incoming floppy disk must be virus-checked.
2. If your anti-virus software finds a virus, tell your PC Support department.

If the rules are broken, users can be 'punished'. Punishment does not work. Users do not believe that you will punish the offenders, especially when you reinforce that belief by not punishing them, because if you do, you will rapidly lose friends and fail to influence people.

Copyright © Dr Solomon's Software

Anti-virus software

What can be done? Anti-virus software is supposed to be the answer, but there are many kinds and many brands. Many users use a scanner, running on any incoming software, or that is what is supposed to happen. In practise, it does not happen. Many files come in that users do not consider need virus checking, for example, Word documents. So, either you try and enforce scanning (procedures that users ignore and 'punish-the-users') or you try and create a situation where everything gets virus-checked.

Users do not always do as they are told, but computers do. So the best idea is to tell the computer to virus-check everything each time it is loaded. This means that programs will be checked more often than necessary, but that is irrelevant.

Virtual device drivers

On a Windows 3.x or Windows 95 machine, you can install an anti-virus Virtual device driver (VxD). A VxD is a 32-bit device driver, which checks everything that arrives on the computer, every floppy disk accessed, every program that is run, and every file that is accessed. You no longer have to rely on the user knowing what to do, that is built into the program. The user interface is simple - the user has to do nothing, just use their computer in the normal manner. If the VxD alerts, then it has found a virus, and an alert is displayed on the user's screen and a network message can be sent to the supervisor. If a virus is found, there is also no option to allow the user to load it. On a Windows NT machine, you can install a File System Driver (FSD), which will provide similar cover.

So, for example, anyone having a problem with the *Concept* virus should install a VxD (or FSD) on all their computers, and tell the network to update it regularly. This will strangle the virus to death.

A VxD will check incoming files no matter where they come from, for example, via the Internet, via the parallel port, or via the floppy drive. Thus there is no point in getting separate products to block each possibility.

No product can scan inside files that are encrypted, where only the user knows the password. Such a file might arrive at the workstation with a virus hidden inside it. If

 Copyright © Dr Solomon's Software

the user never decrypts it, it has no effect, and if the user does decrypt it, then the VxD will alert at that time.

On a machine running DOS, you can run a TSR which has almost the same effect as a VxD under Windows. Word macro viruses cannot work under DOS as there is not a Word for DOS that supports them.

Anti-virus tools

Dr Solomon's recommend that everything be virus checked before it is used – this includes floppy disks with data (remember boot sector viruses) as well as software. This can be done using a scanner (for example, **FindVirus**) which can be installed on every computer (for convenience, because if it is not convenient, it will not get done). Alternatively it can be installed on designated sheep-dip computers, which is more convenient for the PC Support people to keep up to date, but less convenient for the users. Another way is to make the whole thing as transparent and painless as possible by installing a TSR scanner (for example, **VirusGuard**) which means that files are automatically scanned without you being aware of it (unless, of course, a virus is found). The TSR scanner is the route that most people choose, together with some dedicated sheep-dip machines.

Scanners

A scanner is a program that knows how to find a particular repertoire of viruses. Scanners are updated, quarterly or monthly. For many users, quarterly upgrades are sufficient, but every now and then, a new virus comes out and spreads very fast (for example, ***Tequila***, or ***SMEG.Pathogen***). In that case, you could be unable to detect this new virus for several weeks, depending on where you are in the update cycle. Many people subscribe to monthly upgrades to avoid this situation.

Scanners can be either command line, or memory-resident. **FindVirus** is a command line scanner, and must be run by you (this can be done at start-up in the AUTOEXEC.BAT). **VirusGuard** is a DOS memory-resident scanner, and works continuously. As soon as any disk is accessed, it is checked for boot sector viruses, and as soon as any file is used, it is checked for file viruses. Because it is a TSR, there is a slight reduction in free memory (approximately 6Kb) and a slight hesitation each time an executable file is loaded. Also, in common with other TSR scanners, it does not have the full facilities of the command line version (to economize on memory

Copyright © Dr Solomon's Software

consumption), so it cannot carry out a virus CLEAN UP, and it cannot detect a tiny percentage of viruses (the extremely complex polymorphic ones).

WinGuard is a Windows memory-resident scanner (VxD) which takes over from VirusGuard when Windows is run. When both VirusGuard and WinGuard are enabled (as recommended by Dr Solomon's), then control is passed automatically between them as Windows is started up or shut down. Using Windows technology, WinGuard is able to quickly and accurately detect all known viruses, including the complex polymorphic ones.

Checksummers

A checksummer is a change detector. Executable files should not change, except for a good reason, for example, updating of the software. A checksummer aims to detect changes. The advantage of checksummers is that they do not detect a repertoire of viruses, so do not need updating. The downside of checksummers is that they are more hassle than scanners (files change on your computer more often than you might have thought, for good and valid reasons), and also that they do not detect all viruses. For example, checksummers do not detect slow viruses, they do not detect all boot sector viruses (if the hard disk code is left unchanged) and they have problems with stealth viruses. Some people use checksummers, but they are a minority.

 Copyright © Dr Solomon's Software

3. Networks and Viruses

A network is a group of computers connected together to make it easier to share data. This provides interesting opportunities for viruses, and for dealing with viruses.

There is a common perception that once a virus gets onto a network, somehow it flashes round the whole network very quickly. The truth, of course, is more complex. Boot sector viruses cannot travel across networks – if several computers on a network are infected, that is because the virus spread via floppy disks in the usual way. An example of how a file virus spreads across a network is as follows:

1. User 1 gets their computer infected. The virus goes TSR, memory resident.
2. User 1 runs other programs on their hard disk. They get infected.
3. User 1 runs some programs on the network. They get infected. A network emulates a DOS device – reading and writing to files on the server is done in exactly the same way as locally. The virus does not have to behave any differently to infect files on the server.
4. User 2 logs on to the server, and runs an infected file. The virus is now TSR in User 2's computer.
5. User 2 runs several other programs, on their local hard disk, and on the server. Each file becomes infected.
6. User 3, User 4 and User 5 log on and run infected files.
7. And so on.

Macro viruses are especially good at spreading on networks, because people commonly share data across networks, and email documents to each other. They may even share common templates.

Network protection

85% of PC networks use Novell, so we will use that as an example, but you can adapt the same principles for other network operating systems:

1. You can make directories read-only. If you make files on the local hard disk read-only, you are wasting your time, because just about every file virus will make them read/write, infect them, and make them read-only again. This is because the user has the privilege to make files read/write on his local hard disk. But on a file

Copyright © Dr Solomon's Software

server, you do not have to give that privilege to the user, and the virus has the same privilege as the user. Indeed, the virus is the user, and can do no more than the user can – there is no magic about viruses – they are subject to the same constraints as any other programs.

Unfortunately, some packages cannot be run from read-only subdirectories, because they want to write to configuration or temporary files in the same directory.

2. You can make programs execute-only. This means that although the directory is read/write, the executables cannot be written to, or even read. They can only be run. Be warned, though, that on Novell this is a one-way process – once you have made a file execute-only, you cannot go back. All you can do is delete it, even if you are Supervisor. So, make a copy first. Some programs will not run if they are execute only, because they have overlays that are added on to the end of the EXE file. So if the EXE file cannot be read, the overlays cannot be loaded.
3. You can make individual files read-only using the DOS attribute, and then deny the user the 'modify attribute privilege' in that directory.

Using a combination of these techniques, you should be able to make a large percentage of the files on the server uninfectable (indeed, unchangeable without Supervisor intervention). This stops viruses infecting most of the executables on the server. Unfortunately, the important files on the server are the data files, and those you have not protected. The user has read/write access to the data (needed to do the job), and so the virus also has read/write access to the data. Deleting files is the least of the worries – consider that some 'virus damage routines' consist of altering files. So how is the data on the server to be protected? The only answer is to keep viruses off the workstation as well.

Another thing you can do, if your server is Novell based, is run an anti-virus NetWare Loadable Module (NLM) on the server. This can check the files on the server and as they are passed to and from the workstations. It can also be used to prohibit the user from logging on unless they have virus protection in place.

If your file server is Windows NT based, then you can run a Windows NT service to do a similar job.

If your server is Local Area Network (LAN) Manager or LAN Server based, you can run an OS/2 version of the anti-virus program on the server.

 Copyright © Dr Solomon's Software

4. A Brief History of Viruses

1986-1987 — the prologue

It all started in 1986. Basit and Amjad realized that the boot sector of a floppy disk contained executable code, and this code is run whenever you start up the computer with a disk in drive A:. They realised that they could replace this code with their own program, that this could be a memory-resident program, and that it could install a copy of itself on each floppy disk that is accessed in any drive. The program copied itself – they called it a virus. But it only infected 360Kb floppy disks.

In 1987, the University of Delaware realised that they had this virus when they started seeing the label '**(c) Brain**' on floppy disks. That is all it did – copy itself, and put a volume label on disks. This was also the first virus that was seen by Dr Solomon's. A PC Support lady at a university phoned because she was seeing the volume label on a number of disks, and she thought it might be a virus, and because Dr Solomon's was involved in data recovery from disks, she thought Dr Solomon's might be able to help. She sent Dr Solomon's the virus, Dr Solomon's analysed it, and that got Dr Solomon's into the anti-virus business.

Meanwhile, also in 1986, a programmer called Ralf Burger realised that a file could be made to copy itself by attaching a copy to other files. He wrote a demonstration of this effect, which he called ***Virdem***. He distributed it at the Chaos Computer Club conference that December, where the theme was viruses. ***Virdem*** would infect any COM file. Again the payload was pretty harmless.

This attracted so much interest that he was asked to write a book. Ralf had not thought of boot sector viruses like ***Brain***, so his book does not even mention them. But by then, someone had started spreading a virus, in Vienna.

In 1987, Franz Swoboda became aware that a virus was being spread in a program called Charlie. He called it the Charlie virus. He made lots of noise about the virus (and got badly bitten as a result). At this point, there are two versions of the story – Burger claims that he got a copy of this virus from Swoboda, but Swoboda denies this. In any case, Burger obtained a copy, and gave it to Bernt Fix, who disassembled it (this was the first time anyone had disassembled a virus). Burger included the disassembly in his book, after patching out a couple of areas to make it less infectious and changing the payload. The normal payload of ***Vienna*** (or Charlie, as Swoboda called it) is to cause one file in eight to reboot the computer (the virus patches the first five bytes of the code). Burger

Copyright © Dr Solomon's Software

(or maybe Fix) replaced this reboot code with five spaces. The effect was that patched files hung the computer, instead of rebooting. This is not really an improvement.

Meanwhile, in the US, Fred Cohen had completed his doctoral dissertation which was on computer viruses. Dr. Cohen proved that you cannot write a program that can, with 100% certainty, look at a file and decide whether it is a virus. Of course, no one ever thought that you could, but Cohen made good use of an existing mathematical theorem and earned a doctorate. He also did some experiments. He released a virus on a system, and discovered that it travelled further and faster than anyone had expected.

In 1987, Cohen was at Lehigh University, as was Ken van Wyk. So was the author of the ***Lehigh*** virus. ***Lehigh*** was an extremely unsuccessful virus – it never managed to spread far, because it only infects COMMAND.COM and does a lot of damage to its host after only four replications. One of the rules is that a virus that quickly damages its host cannot survive. ***Lehigh*** was nasty. After four replications, it did an overwrite on the disk, hitting most of the File Allocation Table (FAT). But a virus that only infects COMMAND.COM is not very infectious. However, the ***Lehigh*** virus got a lot of publicity, and led to van Wyk setting up the Virus-L news group on Usenet.

Meanwhile, in Tel Aviv, Israel, another programmer was experimenting. His first virus was called ***Suriv-01*** (virus spelled backwards). It was a memory-resident virus, but it could infect any COM file (so could ***Virdem***, but it was not memory-resident), whereas ***Lehigh*** could only infect COMMAND.COM. This was a much better infection strategy than the non-TSR strategy used by ***Vienna***, as it lead to files on all drives and all directories being infected. His second virus was called ***Suriv-02***, and that could infect only EXE files, but it was the first EXE infector in the world. His third attempt was called ***Suriv-03***, and it could handle COM and EXE files. His fourth effort escaped into the world, and became known as the ***Jerusalem*** virus. Every Friday 13th, instead of infecting files that are run, it deletes them. But this date is not common, so the virus is pretty inconspicuous most of the time. It avoids infecting COMMAND.COM, because in those days many people believed that this was the file to watch (see ***Lehigh***).

It looks as if it escaped rather than was released, because it plainly was not ready for release. The author decided to change the way that the virus detected itself in EXE files, and had made part of that change. There is redundant code from the ***Suriv*** viruses still in place, and what looks like debugging code. It was found in the Hebrew University of Jerusalem (hence the name) by Yisrael Radai.

While all this was going on, a young student at the University of Wellington, New Zealand, had found a very simple way to create a very effective virus. One time in eight,

 Copyright © Dr Solomon's Software

when booting from an infected floppy disk, it displayed the message '**Your PC is now Stoned**', hence the name of the virus.

The virus itself was just a few hundred bytes long, but because of its self-restraint and memory-resident replication, it became the most widespread virus in the world, accounting for over a quarter of outbreaks. The virus spread rapidly, because it was inconspicuous (and because in those days, people were keeping a careful eye on COMMAND.COM because of ***Lehigh***). The virus has now almost died out because of the way it infects 3½" which makes its presence obvious (when it was written, there were no 3½" disks).

In Italy, at the University of Turin, a programmer was writing another boot sector virus. This one put a bouncing ball up on the screen, if the disk was accessed exactly on the half hour. It became known as ***Italian*** virus, ***Ping Pong***, or ***Bouncing Ball***. But this virus had a major defect – it could not work on anything except an 8088 or 8086 computer because it uses an instruction that does not work on more advanced chips. As a result, this virus has almost died out (as has ***Brain***, which can only infect 360Kb floppy disks, and which foolishly announces its presence via the volume label).

Back in the US, the ***Yale*** virus appeared. The ***Lehigh*** virus did not make it outside a small circle – neither did the ***Yale*** virus. This was another boot sector virus, but it only copied itself when you booted from an infected floppy disk, and then put another disk in to continue the boot process. No subsequent disk was infected, and if the boot-up continued from a hard disk there was no infection at all.

Also in 1987, a German programmer was writing a very competent virus, ***Cascade***, so-called after the falling letters display that it gave. ***Cascade*** used a new idea – most of the virus was encrypted, leaving only a small stub of code for decrypting the rest of the virus. The reason for this was not clear, but it certainly made it more difficult to repair infected files, and it restricted the choice of search string to the first couple of dozen bytes. This idea was later extended by Mark Washburn when he wrote the first polymorphic virus, ***1260*** (***Chameleon***). Washburn based ***Chameleon*** on a virus that he found in a book – the ***Vienna***, published by Burger.

Cascade was supposed to look at the BIOS, and if it found an IBM copyright it would refrain from infecting. This part of the code did not work. The author soon released another version of the virus, 1704 bytes long instead of 1701, to correct this bug. But the corrected version had a bug that meant that it still did not detect IBM BIOSs.

Of these early viruses, only ***Cascade*** and ***Jerusalem*** are still in the wild.

Copyright © Dr Solomon's Software

1988 — the game begins

1988 was fairly quiet as far as virus writing went. Mostly, it was the year that anti-virus vendors started appearing, making a fuss about what was then only a potential problem, and not selling very much anti-virus software. The vendors were all small companies, selling their software for very low prices ($5 or $10 was common). Some of them were shareware, some were freeware. Occasionally some larger company tried to pop up, but no-one was paying serious cash to solve what was only a potential problem.

In some ways, that was a pity, because 1988 was a very virus-friendly year. It gave ***Stoned, Cascade*** and ***Jerusalem*** a chance to spread undetected, and to establish a pool of infected objects that will ensure that they never become extinct.

It was in 1988 that IBM realised that it had to take viruses seriously. This was not because of the well-known Christmas tree worm, which was pretty easy to deal with. It was because IBM had an outbreak of ***Cascade*** at the Le Hulpe site (in Belgium). IBM found itself in the embarrassing position of having to inform its customers that they might have become infected. In fact, there was no real problem, but from this point on IBM took viruses very seriously indeed, and the High Integrity Computing Laboratory in Yorktown was given responsibility for the IBM research effort in this field.

1988 saw a few scattered, sporadic outbreaks of ***Brain, Italian, Stoned, Cascade*** and ***Jerusalem***, and also the final arguments about whether or not viruses exist. When interviewed, Peter Norton said that they were an urban legend, like the crocodiles in the New York sewers, and one UK expert claimed he had proof that viruses were a figment of the imagination. In 1988, the real virus experts would debate with such people, after that year, they would simply walk away from anyone who had such absurd beliefs.

Each outbreak of a virus was dealt with on a case-by-case basis. Existing software was used to detect boot sector viruses (by inspecting the boot sector), and one-off software was written for dealing with outbreaks of ***Cascade*** and ***Jerusalem***.

In 1988, a virus called ***Virus-B*** was written. This is another virus that does not go memory-resident, and it is a modification of another virus that deletes files on Friday the 13th. When this virus is run, it displays '**WARNING!!!! THIS PROGRAM IS INFECTED WITH VIRUS-B! IT WILL INFECT EVERY.COM FILE IN THE CURRENT SUB DIRECTORY!**'. A virus as obvious as that was clearly not written to spread. It was obviously written as a demonstration virus. Virus researchers are often asked for 'harmless viruses' or 'viruses for demonstration'. Most researchers offer some alternative, for example, an overhead foil, or a non-virus program that does a falling letters display. But it looks as if ***Virus-B*** was written with the intention of giving it away as a demonstration virus – hence the warning. Indeed, it was found that an American

 Copyright © Dr Solomon's Software

company was offering it to 'large corporations, universities and research organizations' on a special access basis.

At the end of 1988, a few things happened almost simultaneously. The first thing was a big outbreak of ***Jerusalem*** at a large financial institution, which meant that dozens of people were tied up doing a big clean-up for several days. The second was that Dr Solomon's gave the first-ever Virus Seminar that actually explained what a virus was and how it worked.

It was clear that Dr Solomon's could not go out and help everyone with a virus. It was also clear that financial institutions, and academic sites, could easily handle a virus outbreak, but they did not have the tools to do the job. All they needed was a decent virus detector, which was not available. So Dr Solomon's wrote one, added some other tools that experience said might be useful, and created the first Anti-Virus Toolkit.

In 1989, the first Friday the 13th was in January. At the end of 1988, it was clear that ***Jerusalem*** was in Spain and the UK, at least, and was in academic as well as commercial sites. Because of the destructive payload within the virus, Dr Solomon's felt that if they failed to send out some sort of warning, they would be negligent. But the media got wind of the story and pursued it. The predictability of the trigger day, together with the fact that it was Friday the 13th caught their imagination, and the first virus media circus was under way.

On the 13th of January, Dr Solomon's had dozens of phone calls, mostly from the media wanting to know if the world had ended yet. But Dr Solomon's also had calls from a large corporate site, a small vendor of PC hardware, and a couple of single users. Dr Solomon's were invaded by TV cameras in droves, and had to schedule them carefully to avoid them tripping over each other. In the middle of all this, the PC Support person from the infected corporate arrived. The TV people wanted nothing better than a victim to film, but the corporate wanted anonymity. Dr Solomon's pretended that he was just one of their staff. Also, at that time, British Rail contacted Dr Solomon's – they had an outbreak of ***Jerusalem***, and they went public on it.

1989 — Datacrime

1989 was the year that things really started to move. The ***Fu Manchu*** virus (a modification of ***Jerusalem***) was sent anonymously to a virus researcher in the UK, and the ***405*** virus (a modification of the overwriting virus in the Burger book) was sent to another UK researcher. A third UK researcher wrote a virus and sent it to another UK researcher – in 1989, the UK was where it was all happening. But not quite all. In 1989,

Copyright © Dr Solomon's Software

the Bulgarians started getting interested in viruses, and Russia was beginning to awaken.

In March of 1989, a minor event happened that was to trigger an avalanche. A new virus was written in Holland. A Dutchman calling himself Fred Vogel (a very common Dutch name) contacted Alan Solomon, and said that he had found a virus all over his hard disk. He said that it was called ***Datacrime***, and that he was worried that it would trigger on the 13th of the next month.

When the virus was disassembled, it was found that on any day after October 12th, it would trigger a low-level format of cylinder zero of the hard disk, which would, on most hard disks, wipe out the File Allocation Table, and leave the user effectively without any data. It would also display the virus's name, ***Datacrime.***
A straightforward write-up of the effect of this virus was published; but it was another non-memory-resident virus, and so highly unlikely to spread.

However, the write-up was reprinted by a magazine, another magazine repeated the story, a third party embellished the story, and by June it was becoming an established fact that it would trigger on October 12th (not true, it triggers on any day after the 12th, until December 31st) and that it would low-level format the whole hard disk. In America, the press started calling it 'Columbus Day virus' (October 12th) and it was suggested that it had been written by Norwegian terrorists, angry because it was Columbus, not Eric the Red, who was attributed to discovering America.

Meanwhile, in Holland, the Dutch police were doing one of the things that police are supposed to do – crime prevention. ***Datacrime*** virus was obviously a crime, and the way to prevent it was to run a detector for it. So they commissioned a programmer to write a ***Datacrime*** detector, and offered it at Dutch police stations for $1. It sold really well. But it gave a number of false alarms, and it had to be recalled, and replaced with version 2. There were long queues outside the Dutch police stations, and lots of confusion about whether anyone actually had this virus (hardly anyone did, but the false alarms muddied the waters).

If the police take something seriously, it must be serious, right? In July, large Dutch companies started asking IBM if viruses were a serious threat. ***Datacrime*** was not, but there was a distinct possibility that a company could get ***Jerusalem, Cascade*** or ***Stoned*** (or ***Italian***, in those days before 8088 computers became a rarity). 'So what is IBM doing about this threat', they asked?

IBM had internal-use-only anti-virus software. They used this to check incoming media, and to make sure that an accident like the one in Lehulpe, Holland could never happen again. IBM had a problem – if they did not offer this software to their customers, they could look very bad if on October 13th a lot of computers went down. The technical

 Copyright © Dr Solomon's Software

people knew that this would not happen, but obviously they knew that someone, somewhere, might have important data on a computer that would get hit by ***Datacrime***. IBM had to make a decision about whether or not to release their software, and they had a very strict deadline to work to – October the 13th would be too late.

In September of 1989, IBM sent out version 1.0 of the IBM scanning software, together with a letter telling their customers what it was, and why they were sending it out. When you receive a letter like that from IBM, and a disk, you would be pretty brave to take no notice, so a lot of large companies scanned a lot of computers, for the first time. Hardly anyone found ***Datacrime***, but there were instances of the usual viruses.

October 13th fell on a Friday, so there was a double event – ***Jerusalem*** and ***Datacrime***. In the US, ***Datacrime*** (***Columbus Day***) had been hyped out of all proportion for a virus that is as uninfective as this one, and it is highly likely that not a single user had the virus. In Europe (especially in Holland) there might have been a few, but not many.

In London, the Royal National Institute for the Blind announced that they had been hit, and had lost large amounts of valuable research data and months of work. Dr Solomon's investigated this particular incident, and the truth was that they had a very minor outbreak of ***Jerusalem***, and a few easily replaced program files had been deleted. Four computers were infected. But the RNIB outbreak has passed into legend as a 'Great Disaster'. Actually, the RNIB took more damage from the invasion of the television and print media than from the virus.

1989 closed with the Aids Information Disk. 20,000 copies of a disk were mailed to users taken from mailing lists, such as the one belonging to PC Business World. The disk came with installation instructions (and a request for $189). If you installed it, it created hidden directories and hidden files, and edited your AUTOEXEC.BAT so that one of these hidden files was run on each boot-up. This counted up to 90 and when it reached that number of boots the trojan would trigger. The trojan encrypted all the filenames on your hard disk, and gave them the hidden attribute, and it looked as if there was only one file on your hard disk, which was an invoice for $189 to be sent to PO Box 7, Panama.

The police investigated the incident, and this led to the arrest and extradition from the US of one Dr. Popp. He pleaded diminished competence, and was allowed to return to the US, but he was also tried in absentia in Italy, where he was sentenced to a prison term.

The main impact of the Aids disk was a major flurry of publicity for malicious software (it was not a virus, but many people did not care about the distinction). Also, a

Copyright © Dr Solomon's Software

surprising number of people installed the software – PC Business World wrote a program to reverse the actions of the disk, and made it available free of charge.

By the end of 1989, there were a couple of dozen viruses that Dr Solomon's knew about, but they did not know that in Bulgaria and Russia, big things were brewing.

1990 — the game gets more complex

By 1990, it was no longer a matter of running a couple of dozen search strings down each file. Mark Washburn had taken the ***Vienna*** virus, and created the first polymorphic virus from it. Dr Solomon's did not use that word at first, but the idea of his viruses (***1260***, ***V2P1***, ***V2P2*** and ***V2P6***) was that the whole virus would be variably encrypted, and there would be a decryptor at the start of the virus. But the decryptor could take a very wide number of forms, and in the first few viruses the longest possible search string was just two bytes long (***V2P6*** got this down to one byte). To detect this virus it was necessary to write an algorithm that would apply logical tests to the file, and decide whether the bytes it was looking at were one of the possible decryptors.

One consequence of this, was that some vendors could not do it. It is not easy to write such an algorithm, and many vendors were, by this time, relying on search strings extracted by someone else. The three main sources of search strings were a newsletter called Virus Bulletin, the IBM scanner and reverse engineering of a competitor's product. But you cannot detect a polymorphic virus this way (indeed, years after these viruses were published, many products are still incapable of detecting these viruses). Washburn also published his source code, which is now widely available. At the time, Dr Solomon's thought that this would bring out a number of imitators. In practice, no-one seems to be using Washburn's code. However, plenty of virus authors are using his idea.

Another consequence of polymorphic viruses is an increase in the false alarm rate. If code is written to detect something that has as many possibilities as ***V2P6***, there is a chance that an innocent file will be flagged, and that chance is much greater than with the sort of virus than can be found with a 24-byte scan string. A false alarm can be more hassle to the user than a real virus, as the user will put all their anti-virus procedures into action.

Also in 1990 Dr Solomon's saw a number of viruses coming out of Bulgaria, especially from someone who called himself 'Dark Avenger'. The ***Dark Avenger*** viruses introduced two new ideas. The first idea is the 'fast infector'. With these viruses, if the virus is in memory, then simply opening a file for reading triggers the virus infection. The entire hard disk is very soon infected. The second idea in this virus is that of subtle damage. ***Dark Avenger-1800*** occasionally overwrites a sector on the hard disk. If this is not

 Copyright © Dr Solomon's Software

noticed for a period of time, the corrupted files are backed up, and when the backup is restored, the data is still no good. ***Dark Avenger*** targets backups, not just data. Other viruses are from the same source, such as the ***Number of the Beast*** (stealth in a file virus) and ***Nomenklatura*** (with an even nastier payload than ***Dark Avenger***).

Dark Avenger was creative about distributing his viruses. He would upload them to BBSs, infecting shareware anti-virus programs, together with a documentation file that gave reassurance to anyone who checked the file size and checksums. He also uploaded his source code so that people could learn how to write viruses.

In 1990, another event happened in Bulgaria – the first virus exchange BBS (VX BBS). The idea was that if you uploaded a virus, you could download a virus, and if you uploaded a new virus, you were given full access. This, of course, encouraged the creation of new viruses, and gets viruses into wider circulation. Also, the VX BBS offered source code, which makes the technology of writing a virus more widely available.

In the second half of 1990, ***Whale*** appeared. ***Whale*** was a very large, and very complex, virus. It did not do very much. Mostly, it crashed the computer when you tried to run it. But it was an exercise in complexity and confusion, and it arrived in the virus researcher's hands like a crossword puzzle to be solved. Some virus researchers wasted weeks unravelling ***Whale***, although in practice you could detect it with a couple of dozen search strings. You did not really need to do any more, as the thing was too clumsy to work anyway. Because it was so large and complex, it achieved fame at the time.

At the end of 1990, the anti-virus people saw that they had to get more organized – they had to be at least as organized as the virus authors. So the European Institute for Computer Anti-virus Research (EICAR) was born in Hamburg, in December 1990. This gave a very useful forum for the anti-virus researchers and vendors to meet and exchange ideas (and virus specimens), and to encourage the authorities to try to prosecute virus authors more vigorously. When EICAR was founded, there were approximately 150 viruses, and the Bulgarian 'virus factory' was in full swing.

1991 — product launches and polymorphism

In 1991, the virus problem was sufficiently interesting to attract the large marketing companies. Symantec launched Norton AntiVirus in December 1990, and Central Point launched CPAV in April 1991. This was soon followed by Xtree, Fifth Generation and a couple of others. Most of these companies were rebadging the programs of other companies (nearly all Israeli). The big problem of 1991 was 'glut'. In December 1990,

Copyright © Dr Solomon's Software

there were between 200 and 300 viruses. By December 1991 there were 1000 (there may have been even more written that year, because by February 1992, Dr Solomon's were counting 1300).

Glut means lots of viruses, and this causes a number of unpleasant problems. In every program, there must be various limitations. In particular, a scanner has to store search strings in memory, and under DOS, there is only 640Kb to use (and DOS, the network shell and the program's user interface might take half of that).

Another glut problem is that some scanners slow down in proportion to the number of viruses for which they scan. Not many scanners work this way, but it certainly poses a problem for those that do.

A third glut problem comes with the analysis of viruses. This is necessary if you want to detect the virus reliably, to repair it, and if you want to know what it does. If it takes one researcher one day to disassemble one virus, then he can only do 250 per year. If it takes one hour, that figure becomes 2000 per year, but whatever the figure, more viruses means more work.

Glut also means many viruses that are similar to each other. This can lead to mis-identification, and therefore a wrong repair. Very few scanners attempt a complete virus identification, so this confusion about exactly which virus is being found, is very common.

Most of these viruses came from Eastern Europe and Russia – Russian virus production was in full swing. But another major source of new viruses was the virus exchange BBSs.

Bulgaria pioneered the VX BBS, but a number of other countries quickly followed. Some shut down not long after they started up, but the Milan 'Italian Virus Research Laboratory' was where a virus author called Cracker Jack uploaded his viruses (which were plagiarized versions of the Bulgarian viruses). Germany had Gonorrhoea, Sweden had Demoralised Youth, America had Hellpit, UK had Dead On Arrival and Semaj. Some of these have now either closed down or gone underground, but they certainly contributed to the glut problem. With a VX BBS, all a virus author had to do was download some source code, make a few simple changes, then upload a new virus, which gave him access to all the other viruses on the board.

1991 was also the year that polymorphic viruses first made a major impact on users. Washburn had written ***1260*** and the ***V2*** series long before, but because these were based on ***Vienna*** they were not infectious enough to spread. But in April of 1991, ***Tequila*** burst upon the world like a comet. It was written in Switzerland, and was not intended to spread. But it was stolen from the author by a friend, who planted it on his father's

 Copyright © Dr Solomon's Software

master disks. The father was a shareware vendor, and soon ***Tequila*** was very widespread.

Tequila uses full stealth when it installs itself on the partition sector, and in files it uses partial stealth, and is fully polymorphic. A fully polymorphic virus is one for which no search string can be written down, even if you allow the use of wild cards. ***Tequila*** was the first widespread polymorphic virus. By May, the first few scanners were detecting it, but it was not until September that all the major scanners could detect it reliably. If you do not detect it reliably, then you miss, perhaps, 1% of infected files. The virus starts another outbreak from these overlooked instances, and has to be put down again, but now there is that old 1%, plus another 1% of files that are infected but not detected. This can continue for as long as you have patience, until eventually the hard disk contains nothing but infected files that the scanner cannot detect. You think that, although the virus came back a number of times, it gradually infected fewer and fewer files, until now you have got rid of it completely, but you are wrong.

In September 1991, ***Maltese Amoeba*** spread through Europe – another polymorphic virus. By the end of the year, there were a few dozen polymorphic viruses. Each of these is classified as 'difficult', meaning that it takes a virus researcher more than a few hours to do everything that needs to be done. Also, most products need some form of hard coding to detect the virus, which means program development, which means bugs, debugging, beta testing and quality control. Furthermore, although a normal virus will not slow down most scanners, a polymorphic virus might.

It was also in 1991 that Dark Avenger announced the first virus 'vapourware'. He threatened a virus that had 4,000,000,000 different forms. In January 1992, this virus appeared, but it was not a virus.

1992 – a very busy year

January 1992 saw the ***Self Mutating Engine*** (***MtE***) from Dark Avenger. At first, all that was seen was a virus that was named ***Dedicated***, but shortly after that, ***MtE*** was seen. This came as an OBJ file, plus the source code for a simple virus, and instructions on how to link the OBJ file to a virus to give you a fully polymorphic virus. Immediately, virus researchers set to work on detectors for it. Most companies did this in two stages. Stage one was look at it and shudder, stage two was ignore it and hope it went away. But at the better R&D sites, stage one was usually a detector that found between 90 and 99% of instances, and was shipped very quickly, and stage two was a detector that found 100%. At first, it was expected that there would be lots and lots of viruses using the ***MtE***, because it was fairly easy to use this to make your virus hard to find. But the virus

Copyright © Dr Solomon's Software

authors quickly realised that a scanner that detected one ***MtE*** virus would detect all ***MtE*** viruses fairly easily. So very few virus authors have taken advantage of the engine.

This was followed by Dark Avenger's ***Commander Bomber***. Before ***Commander Bomber***, you could predict very easily where the virus would be in the file. Many products take advantage of this predictability to run fast. Some only scan the top and bottom of the file, and some just scan the one place in the file that the virus must occupy if it is there at all. ***Commander Bomber*** transforms this, and so products either have to scan the entire file or else they have to locate the virus by following the code.

Another virus that came out at about that time was ***Starship***. ***Starship*** is a fully polymorphic virus (to defeat scanners), with a few neat anti-debugging tricks, and it also aims to defeat checksummers with a very simple trick. Checksumming programs aim to detect a virus by the fact that it has to change executable code in order to replicate. ***Starship*** infects files only as they are copied from the hard disk to the floppy disk. So files on the hard disk never change. But the copy on the floppy disk is infected, and if you then copy that on to a new hard disk, and tell the checksummer on the new machine about this new file, the checksummer will happily accept it, and never report any changes. ***Starship*** also installs itself on the hard disk, but without changing executable code. It changes the partition data, making a new partition as the boot partition. No code is changed, but the new partition contains the virus code, and this is run before it passes control on to the original boot partition.

Michelangelo

Probably the greatest event of 1992 was the ***Michelangelo*** scare. One of the American anti-virus vendors forecast that five million computers would go down on March the 6th, and many other US vendors climbed on to the bandwagon. PC users went into a purchasing frenzy, as the media whipped up the hype. On March the 6th, only 5,000 to 10,000 computers went down, and naturally the US vendors that had been hyping the problem put this down to their timely and accurate warning. It will probably never be known how many people had ***Michelangelo***, but certainly in the days leading up to March the 6th many computers were checked for viruses. After March 6th, there were many discredited 'experts' around.

In August 1992, the first serious virus authoring packages were seen. First the Virus Creation Laboratory (VCL) from Nowhere Man, and then Dark Angel's Phalcon/Skism Mass-Produced Code Generator. These packages made it possible for anyone who

 Copyright © Dr Solomon's Software

could use a computer to write a virus. Within twelve months, dozens of viruses had been created using these tools.

Towards the end of 1992, a new virus writing group called Association of Really Cruel Viruses (ARCV) had appeared in England – within a couple of months, the Computer Crime Unit of New Scotland Yard had tracked them down and arrested them, with considerable help from the anti-virus community. ARCV flourished for about three months, during which time they wrote a few dozen viruses and attracted a few members.

Another happening of 1992 was the appearance of people selling (or trying to sell) virus collections. To be more precise, these were collections of files, some of which were viruses, and many of which were assorted harmless files. In America, John Buchanan offered his collection of a few thousand files for $100 per copy, and in Europe, The Virus Clinic Unit offered various options from £25. The Virus Clinic was raided by the Computer Crime Unit after its first (and only) advert in Micro Computer Mart.

1993 — polymorphic viruses and engines

In 1993, the Crypt newsletter blew the whistle on the US Government. They said that the Department of Treasury, Bureau of Public Debt, ran a BBS called the AIS board. From this, it was possible to download the source code of several hundred viruses, and there was no check made on the identity or motives of the callers. This story was checked and found to be true, and it was announced at the Ides of March Virus Conference in New York. Not very much happened until June, when a US citizen again blew the whistle, and there was a front page article in the Washington Post. This embarrassed the US Government into admitting that it was perhaps not a good idea to make such material publicly available, and the 'dangerous material' (together with a large amount of useless harmful information) was removed.

Early in 1993, XTREE announced that they were quitting the anti-virus business – the first time that a major company had given up.

Also early in 1993, a new virus writing group appeared in Holland, called Trident. The main Trident author, Masud Khafir, wrote a polymorphic engine called the ***Trident Polymorphic Engine*** (TPE), and released a virus that used it called ***GIRAFE***. This was

Copyright © Dr Solomon's Software

followed by updated versions of ***TPE***. The ***TPE*** virus is much more difficult to detect reliably than the ***MtE***, and very difficult to avoid false alarming on.

Khafir also released the first virus that worked according to a principle first described by Fred Cohen. The ***Cruncher*** virus was a compression virus that automatically added itself to files in order to auto-install on as many computers as possible.

Meanwhile, Nowhere Man of the Nuke group had been busy. Early in 1993, he released the ***Nuke Encryption Device*** (***NED***). This was another mutator that was more tricky than ***MtE***. A virus called ***Itshard*** soon followed.

Phalcon/Skism was not to be left out. Dark Angel released ***DAME*** (***Dark Angel's Multiple Encryptor***) in an issue of 40hex – a virus called ***Trigger*** uses this. Trident released version 1.4 of ***TPE*** (again, this is more complex and difficult than previous versions) and released a virus called ***Bosnia*** that uses it.

Soon after that, Lucifer Messiah, of Anarkick Systems had taken version 1.4 of ***TPE*** and written a virus ***POETCODE***, using a modified version of this engine (1.4b).

Also early in the year another highly polymorphic virus appeared called ***Tremor***. This rocketed to stardom when it got included in a German TV broadcast of software (received through a decoder). The infected file was PKUNZIP.EXE, which most recipients used to decompress the files they received.

In the middle of 1993, the Trident group got a boost when Dark Ray and John Tardy joined the group. Tardy released a fully polymorphic virus in 444 bytes.

The main bad news of 1993 was the emergence of an increasing number of polymorphic engines and proliferation packages, which make it easier to write viruses that scanners find difficult to detect.

Also in 1993, more significant anti-virus companies disappeared – Certus (whose products included Novi) were taken over by a competitor. Fifth Generation, whose product was called Untouchable, also disappeared.

There was some good news, though. Dr Solomon's Software received the Queen's Award for Technological Achievement. This was awarded for the virus description language, VIRTRAN which is at the heart of the **FindVirus** and **VirusGuard** Anti-Virus scanners.

 Copyright © Dr Solomon's Software

The Generic Decryption Engine

The ongoing glut of viruses written using virus packages presented a major problem for the anti-virus authors who were already hard pressed. It became necessary to mechanize the analysis.

The solution was the Generic Decryption Engine (GDE), which decrypts the code of a suspect file, leading to a firm decision whether it is a virus or not. This eliminates the danger of giving false alarms on such viruses – once the virus is decrypted, it is easy to make a positive identification of the virus.

1994

In April of 1994, Central Point Software ceased to exist. Central Point was one of the major players in the anti-virus market with their CPAV product.

1994 also saw a bigger virus glut than any previous year, from 4000 at the start of the year to 6000 at the end. The viruses came from all over the world, including Australia, China, Russia, India and the Far East. Active European virus writing groups included Immortal Riot (Sweden) and Grog (Italy), but the viruses they produced were easy to handle.

The Far East had started to produce Mutation Engines, including ***DSME*** from Dark Slayer. Bulgaria produced very little, and Dark Avenger, nothing.

The effect of the glut was to place a severe strain on the anti-virus vendors, who had to step up their code output, or fall behind. The process could be handled by increasing the programmer resource, or by introducing industrial engineering techniques, or by a combination of both. Dr Solomon's chose the combination and kept up with the glut.

It was also noticed that a number of new viruses apparently came from the North West of England. The author (or authors) seemed to specialize in companion viruses, which introduce an additional (hidden) file, for each file they infect. The original usually remains unaltered, which defeats change detectors.

In 1994, three viruses in particular gave a lot of trouble, and are worth specific mention.

Natas

Natas (Satan spelled backwards) is the most successful American virus ever released. It appeared on bulletin boards in early 1994 and is rampant worldwide, but particularly in Mexico. It is extremely polymorphic, and also multipartite, which means that in addition to infecting files, it also infects boot sectors of floppy disks, and partition

Copyright © Dr Solomon's Software

sectors of hard disks. A user who fails to clear up all three infections, finds that they keep coming back. This factor, and the fact that second rate products fail to detect all instances, mean that the virus can quickly spread.

It is believed that the author is now employed by an American anti-virus organization, and was disgusted to find how easy it was to write the code to detect the virus, and repair the infected files.

The virus type is also called SPaM (Stealth, Polymorphic And Multipartite).

One-Half

Written in Czechoslovakia, this virus must rank (so far) as the most difficult for anti-virus vendors to handle. Dr Solomon's, who normally provide next-day service to detect a new virus, needed to develop a new tool to detect ***One Half***, and responded seven weeks later. Others took much longer. The virus had a 3-month honeymoon period, and became rampant, first in Czechoslovakia, and then worldwide.

The virus infects files, using ten 'islands of code' scattered around the end of the original file. These have to be followed, so as to detect reliably, and they have to be replaced, if the file is to be repaired.

One Half infects the partition sector of the hard disks, in addition to the files, and has another nasty habit. Every time that the user boots from the infected hard disk, the virus encrypts cylinders of the hard disk, starting one cylinder from the end, and working backwards. It keeps a record of the last (lowest) cylinder that it encrypted, in the infected partition sector. When it has encrypted half of them, it displays the message '**Dis is one half**', which gives the name.

As long as the user continues to use the infected machine, the virus decrypts encrypted cylinders 'on the fly', and the PC remains useable. If the user cleans up the partition sector, without first copying the files to an external device, the data on the encrypted cylinders is lost.

SMEG.Pathogen

When it was released, this virus brought a great deal of trouble for two UK organizations. Whereas earlier polymorphic viruses had decryptors that were less than 200 bytes long, this one had a 2Kb decryptor, of which 95% was executable rubbish. This made it very difficult to detect. The author deliberately infected a shareware anti-virus

 Copyright © Dr Solomon's Software

product on a bulletin board for downloading, and users who thought that they were getting a good anti-virus product, got it with the virus, which the product did not detect.

The author, an unemployed Englishman called Christopher Pile (he called himself "The Black Baron"), followed up with a further development – ***SMEG.Queeg***, and then he published the SMEG polymorphic engine. He was apprehended by the Computer Crime Unit in late 1994, charged, and later convicted of eleven offences against the Computer Misuse Act. In 1995, he was sentenced to eighteen months in prison.

1995

On the 26th May 1995, Christopher Pile, 26, of Plymouth in England, was convicted under the Computer Misuse Act in connection with the ***Smeg*** viruses.

In 1995, the glut continued. There were 7,000 viruses and variants by mid-1995, and anti-virus vendors were still feeling the strain. Viruses from the Far East included hacks of some of the classics, for example, the Mad Satan of Taiwan, produced a range of CVEX viruses, which on examination, were clearly descended from ***Jerusalem.***

Polymorphics abounded. There were also the VICE viruses and the ***Pinworm*** viruses, both from an author called Virogen. It was evident that the days when anti-virus vendors could avoid the issue, and not detect this type of virus in a proper manner, would soon be gone.

Advanced Heuristic Analysis (AHA)

In mid-1995, Dr Solomon's introduced Advanced Heuristic Analysis, whereby the use of the /ANALYZE switch allowed FindVirus to check for probable new viruses (as yet unseen).

The early detection of new viruses hastens the inclusion of these new viruses in full identification mode, enabling repair to take place.

WM.CONCEPT

August 1995 saw a significant new development, the first macro virus.

WM.Concept infects Word for Windows 6 documents [*.DOC] and the NORMAL.DOT template. The virus makes use of the well-developed Word for Windows macro language, Word Basic, in an attempt to exploit the fact that PC users exchange documents far more often than programs. When an infected document is opened under

Copyright © Dr Solomon's Software

Word for Windows for the first time, the virus gets control as an AutoOpen macro and infects the NORMAL.DOT template [or any other template, if it has been selected as a global default template]. A Word for Windows message box, with the text **1**, appears on the screen. After this, every document saved using the File ¦ SaveAs command is infected with the virus. This normally happens when a newly-created document is saved to the disk. If Word for Windows is run, then Tools ¦ Macros is selected and the list of macros checked, the presence of the macros named AAAZFS, AAAZAO, AutoOpen, PayLoad and FileSaveAs indicates that the Word for Windows system is infected with the WM.Concept.

The implications of this simple development (which had long been foreseen by the anti-virus community, who had hoped it would never happen) are far-reaching.

Macro viruses [such as WM.Concept] seem likely to become a significant threat, for several reasons.

(1) Macros, written in WordBasic, and accessible to many computer users, are easier to write than 'traditional' file viruses [written, for the most part, in assembly code].

(2) They are the first viruses to infect data files, rather than executables. Data files, to which macros are attached, provide viruses with a more effective replication method than executable files. Data files are exchanged far more frequently than executable files. This coupled with the increased use of e-mail [and the ability to attach files to e-mail], and mass access to the internet [and on-line services like CompuServe and America Online], is likely to make macro viruses a much greater threat to computer users than 'traditional' file viruses.

(3) Macro viruses are not platform-specific. There are versions of Microsoft Word for Windows 3.x, Windows 95, Windows NT and Macintosh. This makes all of these operating systems susceptible to macro viruses [although anything in a macro which makes use of calls to a specific operating system, as with the WM.FormatC macro trojan, will be restricted to that particular operating system].

Macro viruses have already had a marked effect. WM.Concept currently [July 1996] accounts for around 50% of all virus reports to Dr Solomon's Technical Support department. While WM.Concept causes no damage to data, we have already see the first [albeit faltering] steps towards macro viruses which threaten data; one payload of WM.Nuclear, for example, is to attempt to damage the system files [this payload is never delivered, due to a bug in the code].

Macro viruses are not confined to Microsoft Word for Windows. In January 1996, the first macro virus to infect Lotus AmiPro files [APM.GreenStripe] appeared. Unlike Word for Windows, in which macros are directly linked to DOC [and DOT] files, AmiPro

 Copyright © Dr Solomon's Software

macros are contained in a separate file [with the extension SMM]; this makes it possible to exchange AmiPro documents [for example, via e-mail] without exchanging infected macros. XM.Laroux, which appeared in July 1996, is the first working macro virus to infect Microsoft Excel for Windows spreadsheets.

The future

There will be more viruses – that is an easy prediction. How many more is difficult to predict. There were over 8,000 viruses by the middle of 1996 and this figure is expected to be 11,000 by the end of 1997.

The glut problem will continue. Whenever a group of serious anti-virus researchers meet, they find an empty room, hang 'Closed for cleaning' on the door, and frighten each other with 'nightmare scenarios'. Some of the older nightmare scenarios have already come true, others have not, but remain possibilities. The biggest nightmare for all anti-virus people is glut. There are only between 10 and 15 first class anti-virus people in the world, and most of the anti-virus companies have just one of these people (some have none). It would be difficult to create more, as the learning curve is very steep. The first time that an anti-virus researcher disassembles something like ***Jerusalem*** virus, it takes a week. However, after they have done a few hundred viruses, they could do something as simple as ***Jerusalem*** in 15 minutes.

The polymorphic viruses will get more numerous, and more complex. The need to detect them all will be a serious problem for anti-virus packages without GDE capability. They are a much bigger problem than the stealth viruses, because stealth is aimed at checksummers, but polymorphism is aimed at scanners, which are what most people are using. Each polymorphic virus will also be a source of false alarms, and will cause the researchers much more work than the normal viruses.

The databases that scanners use will get larger. Each new virus needs to be detected, identified and removed. Loading the databases will take longer, and some programs will have memory shortage problems.

As Windows 95 and Windows NT become popular, users will be increasingly reluctant to run scanners under DOS. But to run Windows, you have already run software on the hard disk, and if one of the things you have run is infected by a virus, you have a virus in memory. If there is a virus in memory, you cannot trust what the computer is saying –

Copyright © Dr Solomon's Software

it could be a stealth virus. In other words, Windows will make anti-virus software less secure.

The R&D effort to keep scanners up-to-date will continue to increase. Some companies will not be able to do it, and will decide that scanning is outdated technology and try to rely on checksumming. Other companies will license scanners from one of the few companies that still maintain adequate R&D (some of this has already started to be seen). Some companies will decide that the anti-virus business is not as profitable as they had thought, and will abandon their anti-virus product and go back to their core business.

Users will get a lot more relaxed about viruses. The stage has long since passed where a virus is regarded as a loathsome disease, to be kept secret. But people are increasingly being seen who regard a virus on their system with about the same degree of casualness as a bit of fluff on their jacket. Sure, they will wipe it off, but there is not a real need to worry about it happening again. This is perhaps a bit too relaxed an attitude, but what else can be expected if a user keeps on getting hit by viruses, and nothing terrible ever seems to result.

Anti-virus products will mature a lot. Those without a friendly decent user interface will have a hard time competing against the pretty ones. Those with a long scan time will be rejected in favour of those that scan in seconds. Exactly which viruses are detected will have far less emphasis (it is very difficult for users to swallow claims about so many thousands of viruses) than the ease of use of the product, and the amount of impact it has on the usability of the computer.

New products will keep arriving as each company invents the product that makes all previous products obsolete. Sometimes the magic ingredient will be software (AI, neural nets, whatever is the latest buzzword) and sometimes it will be hardware (which can never be infected, except that is not the problem). These products will burst on a startled world in a blaze of publicity, and vanish without trace when users find that installing them makes their computer unusable, or else it does not find any viruses, or both. But new ones will come along to take their place.

Gradually, people will trade up from DOS to whatever takes its place – OS/2, Windows 95, Windows NT or UNIX, and the DOS virus will become as irrelevant as CPM. Except that DOS will still be around 10 years from now. Operating systems are being promoted as secure, but the computers that they are installed on are not secure against viruses, any more than they are secure against theft. It is extraordinarily difficult to write an

 Copyright © Dr Solomon's Software

operating system that is virus-proof without it also being useless for most other purposes.

Some computers are already being built with ingrained resistance to viruses. Some brands of computer are already immune to boot sector viruses, provided you make a simple choice in the CMOS setup (do not boot from the floppy disk). Right now, very few users are being told that these computers can be set up that way, but people are gradually finding out for themselves. This does not solve the virus problem, but anything that makes the world a difficult place for viruses must be a help.

The virus problem will be with us for many years to come. It is not the dramatic, world-shaking kind of problem that ***Michelangelo*** was made out to be. Nor is it the 'fluff-on-your-jacket' kind of problem. But as long as people have problems with computers, other people will be offering solutions for those problems.

Copyright © Dr Solomon's Software

 Copyright © Dr Solomon's Software

5. Mechanisms of Stealth

For a virus to be a virus, all it needs to do is copy itself. But to be a successful virus, it needs to be as inconspicuous as possible. Like a mouse, its main defense is that you do not know that it is there, because as soon as you spot it you will attempt to kill it.

The generic term for the attempt to remain inconspicuous is stealth, but there are various degrees of stealth and various mechanisms for achieving this. Overall, there has been an increasing trend in this direction. This chapter discusses some of the reasons.

Some technical information is also provided in this chapter. This is of no use to virus authors, as it is all published in standard reference manuals, for example, the MS-DOS Encyclopedia, published by Microsoft Press.

Some viruses are highly visible. For example the ***Burger*** viruses overwrite the beginning of the file that they infect, the program no longer functions and you immediately notice that fact. There is absolutely no way that you can fail to notice an overwriting virus. This is called negative stealth, level -1. About 10% of viruses have negative stealth, and the obvious question is why? The reason must be that there is a segment of virus authors who really do not care about writing a virus that actually is survivable. All they want is the nice warm feeling that comes with being able to boast that they have written a virus. Boot sector viruses cannot have negative stealth – if they did not pass on control to the original boot sector, the computer would not boot up at all.

The next level up is really necessary in order for the virus to spread at all. The original program must still run, or substantially so. This is done by adding the virus to the file, yet preserving all the necessary information for the program still to run, and for the virus to execute in addition to the original program. Approximately 90% of viruses do this. We call this stealth level 0. But if the virus does no more than this, it will be only moderately noticeable because people do not look at time-stamps.

Just in case they do (many magazines advocate this as an anti-virus measure), most viruses implement stealth level 1, or elementary stealth:

1. If date and time are not preserved during the infection, an increasing number of programs will have a current time stamp. This might be noticed by an alert user, and is certainly visible if you look out for it. It is avoided by using interrupt 21h,

Copyright © Dr Solomon's Software

function 57h, although there are some viruses that use lower-level methods to preserve the date and time.

2. If a virus uses DOS-writes to add itself to the file, and the disk is write-protected, DOS will give a critical error '**Abort, Retry, Fail**'. This will be noticed – you may ask why the disk is being written to, when all you did was try to run a program. Again, it would need an alert user to spot this, and anyway write-protected media does not get used very much. It is fairly easy to avoid this problem. The critical error comes to you via interrupt 24h, and it can be replaced temporarily with a small routine that does nothing at all. Boot sector viruses do not have to do anything about these issues.

In addition, to qualify for stealth level 1, the virus must do nothing flashy to call attention to itself. For example, the ***Diamond*** (***V1024***) virus displays every hour, on the hour. A multicolored diamond pops up on the screen, shatters into diamond fragments which then dance around the screen, gradually clearing it. Thus you are sure to notice that something odd is going on.

At stealth level 2, intermediate stealth, things start to get more interesting. Below that level, the virus can be seen with the naked eye, as it were. For a file virus, you could see the difference in file size, or in the case of a boot sector virus you would see a peculiar boot sector. It is possible to conceal the increase in file size, and this can be done in a number of ways. The most obvious way is not to have an increase in file size in the first place. The ***Zero-hunt*** virus looks for a block of contiguous zeros in the file, and if it finds this it overwrites that part of the file with itself. The file, therefore, does not grow at all. When the infected program runs, the virus runs first, and after going memory-resident it overwrites the memory image of the file with zeros so that the program will run completely normally. The ***Rat*** uses a similar technique, but only works in EXE files, where it looks for the block of zeros that many compilers put at the start of the EXE file just after the header.

For many users, the only method they use to inspect file sizes is with a DIR command. DIR uses interrupt 21h, functions 11h and 12h. If the virus intercepts interrupt 21h and traps these functions, it can subtract the length of the virus from the returned value, and pass this fake value on to any calling program. So DIR looks normal. ***Zero-Eater*** (also called ***Zero-bug***) uses this technique.

A second method to find out file size is interrupt 21h, functions 4eh and 4fh. These are the handle equivalents of 11h and 12h, and some of the programs that act as a user shell for DOS use these calls to find out file sizes. Also, if an anti-virus program

 Copyright © Dr Solomon's Software

is checking on file sizes, it probably uses these functions as they are easier on the programmer than 11h and 12h. The virus can also trap and fake these calls.

A third method to find out file size is interrupt 21h function 42h subfunction 2. This is seek to end-of-file, and the file size is returned in the registers. A sneaky anti-virus program might use this call to determine the file size, but there are also sneaky viruses that do their subtraction on this, for example, ***Tequila***.

Of course, you can avoid such tricks by cold-booting from a known clean DOS disk which is what Dr Solomon's tell users to do. Of course, the number of users who actually do this before running their anti-virus software can be counted on the fingers of one hand. It has to be assumed that users do not do as instructed because a lot of them did not read the manual, but many of those that did, decided that it was not necessary to do what they had been told.

One problem with these three methods is that the virus must be in memory for the stealth to operate, and maybe the virus has not yet been run, or maybe the user has cold-booted from a clean DOS disk. The next way to avoid the apparent growth in file size is to increase the file size, but not let the directory entry show this. The ***Number of the Beast*** virus is 512 bytes long, and replaces the first sector of the file with itself. But it needs that original sector, so it stores it after the end of the file, in the space between the end of the file and the end of the cluster. Many hard disks have 2Kb clusters, so approximately 75% of files will have the necessary available space. A problem with this approach is that when you copy that file on to a floppy disk, the cluster size will be 1Kb at most, and high-capacity floppy disks have a cluster size of 0.5Kb. When you copy an infected file on to a floppy disk the virus will be copied, but not all of the original program. ***Number of the Beast*** has been seen in the wild in Western Europe, but not in the USA.

The ***V1963*** virus (and ***V1963B***, also called ***Necrophilia***) needs 1963 bytes, so the previous technique would not be very successful. Instead, it adds one cluster to the FAT chain and uses that cluster to store the first 1963 bytes of the original file. Therefore, even if the virus is not in memory and the directory entry is left unchanged, the file size does not look suspicious.

In the case of boot sector viruses, for the virus to be intermediate stealth, it would have to show the original boot sector whenever a request is made to read the boot sector. ***Brain*** was the first virus that did this. But the fact that it readily puts a volume label '(c) Brain' on the disk, plus the noticeable 3Kb in bad sectors on the disk, disqualifies it from being intermediate stealth.

Most of the so-called stealth viruses in many virus catalogues are actually intermediate stealth. Very few intermediate stealth viruses are successful. Since very

Copyright © Dr Solomon's Software

few users go looking for viruses, the benefit of intermediate stealth over elementary stealth is not really as great as it would seem. To reap real benefits from invisibility it is necessary to go to advanced stealth. In advanced stealth, the virus aims to be invisible to anti-virus programs. First, however, we shall cover a few assorted stealth tricks.

Assorted stealth techniques

Certain anti-virus programs work by intercepting the interrupts and blocking naughty attempts, such as the attempt to write to COM or EXE files. If such a program is in memory, it is clearly a good idea to disable it before the virus infects anything. One well-known anti-virus program, in some versions, provided a convenient way for a virus to do this, so that a user wishing to perform some action that would normally be flagged as suspicious, can do so without raising a false alarm. Some viruses, such as ***Eight Tunes***, detect this product by using its own 'Are you there?' call.

Another technique that is sometimes seen was prompted because many scanning programs do a self-check before running, and if there is any change to the file they report it. This would mean that a new virus might be detected in this way. So some of the viruses refrain from infecting such programs. One common way this is done is to look for the letters SC or SCAN at the beginning, or alternatively anywhere, in the filename. Another string that they avoid is a file with TEST in the name. You might consider renaming your scanner, although it might object to this.

Viruses that stealth the file size often leave an inconsistency between the size according to the directory entry and the number of elements in the FAT chain. When CHKDSK is run, it will report these inconsistencies, and CHKDSK is a program that is often run when problems are suspected. To avoid a suspicious report by CHKDSK, at least one virus checks the name of the program being run, and if it is CHKDSK, the file size stealth is disabled.

Advanced stealth

A virus that uses advanced stealth is aiming to conceal its existence even from anti-virus software. The best known example of this, ***Frodo*** (also known as ***4096***, ***4K*** and ***IDF. Frodo***), is much misunderstood. Reports have been seen that it disinfects itself when read, which is a rather curious way of describing what it actually does. In fact, it traps interrupt 21h, and when any file-related operations are performed it starts.

Copyright © Dr Solomon's Software

When any program uses DOS to read, write, seek or whatever in the file, ***Frodo*** works out what that DOS call would have seen if the file had not been infected, and returns that information for DOS to present to the calling program. The result is that with ***Frodo*** in memory, even if you do a byte-by-byte comparison between an infected file and a clean copy (on a write-protected floppy disk), the comparison would report no difference. ***Frodo*** marks files by adding 100 years to the date stamp (hence the alias 100 years, and even the existence of this is concealed). As a result, it is difficult to notice that ***Frodo*** is present, and it's tricky to get rid of it.

Frodo has a neat way of concealing itself in memory, too. Most programs that go memory-resident and capture an interrupt do so by changing the entry in the Interrupt Vector Table (IVT). As a result, some people have guessed that this is the only way to do this. But ***Frodo*** avoids this method to fool programs that check for changes in the IVT. Instead, ***Frodo*** patches the first five bytes of the interrupt handler with a jump to the ***Frodo*** code. After the ***Frodo*** code is run, it then re-patches the original DOS kernel back to what it was before, and jumps to it.

Number of the Beast (so called because of the 666 in the code) is exactly 512 bytes long (there are approximately a dozen versions of it now). It is also an advanced stealth virus, but it does this trick by manipulating the system file tables inside DOS. The 512 bytes of the virus are very tightly coded – it looks like a Swiss watch, although perhaps that should be a Bulgarian watch. If there is any attempt to read the first 512 bytes of an infected file while the virus is in memory, it fetches the original 512 bytes that it has placed after the end of the file, and presents those instead. Again, DOS Compare and cryptographic checksummers are fooled into thinking that the file is unchanged from the original.

Number of the Beast also has a neat way of hiding in memory. It needs precisely 512 bytes of storage, and it gets this by taking the first DOS buffer, and convincing DOS that the second buffer is actually the first. Thus, most memory mappers will not recognize this 512 byte hole in memory, or else think that it is part of DOS.

Amongst boot sector viruses, ***Joshi*** and ***EDV*** use advanced stealth techniques. With either of these viruses, if the virus is in memory and you look at the sector that contains the virus code, the virus redirects the read to where it put the sector that it replaced, so that anti-virus software sees nothing amiss. ***EDV*** has some additional tricks. If you look at the place where it located the sector it replaced, at cylinder 39, head 1, sector 8, the virus returns an unreadable sector error, so that you do not see a boot sector in such an unusual place. When the virus goes memory-resident, it first

Copyright © Dr Solomon's Software

tries to use any memory above 640Kb, if available, so that memory mappers do not see it.

Joshi will survive a (Ctrl Alt Del) combination. Most people think that (Ctrl Alt Del) triggers a re-boot. Actually it is just another keystroke that can be replaced by replacing interrupt 9. This trick of ***Joshi*** has allowed it to survive clean-up operations by users who think that all you have to do is reboot and low-level format hard disks – not only is this overkill, but it also does not necessarily do the job, unless you do the right things in the right order.

Today, a great many of the viruses in the world are stealth boot sector viruses.

Copyright © Dr Solomon's Software

6. Polymorphic Viruses

The main enemy of viruses is the scanner. This is because it is the only tool that many people use (indeed, many users seem to believe that it is the only possible tool). So virus authors have developed ways of concealing the existence of the virus from scanners, or at least making it more difficult for the scanner to detect them.

Perhaps the first virus that started to do this, was ***Cascade***. Most of the virus is encrypted using two variable encryption keys. The only constant part of the virus is the decryptor/loader, which is a couple of dozen bytes of code that decrypts the rest of the virus so that it can run. This means that the designer of the scanner has only a couple of dozen bytes from which to choose the search string, and there is a lovely and obvious sequence to choose – 141$Flu. In the early days, many scanners chose this sequence, but failed to encrypt the search string in the scanner itself. As a result, scanners would find this string in each other, and give false alarms. These days, nearly every scanner encrypts all its search strings to avoid this problem. There are still a few that do not, or which fail to clear them from memory after running, which leads to false alarms. Because ***Cascade*** has only a few dozen bytes which are not encrypted this problem is aggravated.

The next step was when the virus authors started putting some variable bytes in the middle of the decryptor/loader. These bytes do nothing of significance, so can be any valid instruction, but this means that the scanner has to implement wildcard searches which adds some complexity to the program. ***Phoenix, Evil, Proud*** and ***Virus101*** use this technique.

What followed was to include a number of non-significant instructions in the virus. To do this, a random number generator chooses the non-significant instruction, and chooses the number of these instructions to be used. At this point, the possibility is a code generator in the body of the virus to generate different randomized decryptor/loaders. The ***Simulate*** virus uses this technique. It means that the virus researcher has to implement a search engine that is capable of accepting a wildcard which represents a variable number of bytes within certain limits. What are those limits? The virus researcher needs to know, because if there are, for example, six 3-byte search strings and these are allowed to occur within 64Kb of file, the probability of a false alarm is much greater than if the specification is that they must all occur within 100 bytes. But until the virus has been disassembled, analyzed and understood, this prediction cannot be made.

Copyright © Dr Solomon's Software

Then virus authors realized that in many code sequences the exact order of the instructions does not affect the outcome. For example, if you load the AX register and then the CX register, the outcome is the same as if you load CX and then AX. So if a code generator is written to randomize the order of the instructions, it is made even harder for the virus researcher to search for the virus. The virus researcher either has to give the search engine a great many search strings or has to have some way of telling the scanner that, within certain limits, the order of finding these fragments does not matter. Again, the researcher has to disassemble and understand the virus before being able to predict the limits of the code generator. Yet again, the search engine must be more complex. ***Maltese Amoeba*** uses the above technique, which is why it is tricky to detect accurately.

The next step was to realise that there are many completely different code sequences that accomplish the same end. For example, to copy the CS register into the DS register, you can:

```
Push CS
Pop  DS
or
Mov AX, CS
Mov DS, AX
```

And so on. Again, this can be implemented by the code generator. ***Tequila*** uses this method. Another trick was to realize that many of the registers on the 8088 can be used interchangeably for each other. So, instead of using AX to contain the decryption key, you can use, for example, DX, DI or SI. Changing the register that is used changes one of the bytes in the decryption routine. The Washburn viruses ***1260***, ***V2P1***, ***V2P2***, ***V2P6*** and ***V2P6Z*** use these techniques. In the ***1260*** virus the longest available search string is two bytes long; there are not many of them, and they occur in many different orders. ***V2P2*** is the same, and the number of bytes added to the original file is variable. In ***V2P6*** the longest available search string is one byte long, and there are about half a dozen of these constant bytes which can occur in many different positions and in many different orders. The source code of these viruses is available on the virus exchange BBSs, so anyone who wants to learn the technique can do so. Where the source code is not available, there are disassemblies that you can download.

The virus researcher has great difficulty in scanning for such a virus. The code generator in the virus has to be disassembled, analyzed and understood, and this might not be as easy as it sounds. But once it has been done, the relationships between the bytes can be determined (rules like, for example, if the byte at offset 14 is

 Copyright © Dr Solomon's Software

a 67 then the byte at offset 19 must be a 73). Finally, a subroutine can be written that can be linked into the software and detect the virus in all its instances. This involves hard-coding the scan, as opposed to using search strings, which is more difficult and bug-prone. If the smallest mistake is made, innocent files may be accused of harbouring the virus, or one or more instances of the virus may fail to be detected. Which means that the virus survives the clean-up. It also means that, a search string for these viruses cannot be published.

Each virus that uses such a sophisticated decryptor/loader causes an immense amount of work for the scanner vendor, and some of the vendors are beginning to give up. Of course, this is another encouragement to the virus authors to use such techniques. WonderScan (with apologies if there really is such a product) may fail to detect any viruses that fall into this category. So any virus author that wants a virus to spread unimpeded only has to use a complex code generator of this kind to ensure that the virus spreads widely. However, despite the difficulties, many vendors are still continuing.

The stage has been reached where it is necessary for the virus researcher to disassemble, analyze and understand the virus code generator. Thus the virus authors can make it more difficult for them to do so. This technique is used in ***Virus-101***. Some of the code is written in a very obscure way, and uses features of the 8088, for example, segment wraparound. Another technique is to make stepping through the code more difficult. One virus uses the 8088 pipeline, so that if you step through the code the computer reboots, but if you run the virus, that instruction is a simple jump to the next instruction. That is not a problem. Nor is the technique of disabling the keyboard as you step through the code, leaving you with a dead computer that you have to reboot.

The ***1260***, and the ***V2*** series use another method. Under the first layer of encryption there is a second layer. A few dozen of the bytes in the virus are encrypted with another encryption routine, such that if you simply disassemble after the first decryption, the important parts of the virus make no sense. So you have to deal with the second layer of decryption, and you cannot do that by simply stepping through the code with the Debug debugger.

The way that Debug (and other debuggers) work is by putting a single-byte interrupt (interrupt 3, 0cch) into the code, and saving the byte that used to be there. When the program reaches that point, the interrupt 3 is executed, which stops the execution and triggers Debug's display. Another method that Debug uses is to put the processor into single-step mode, and then every instruction executed also causes an interrupt 1, which can be programmed to do whatever is required, for example,

Copyright © Dr Solomon's Software

display the contents of the registers. So Debug needs to use interrupts 1 and 3. ***1260*** and the ***V2*** series to use these interrupts to do the second layer of decryption. ***Tenbytes*** does the same, and the ***Fichv*** series from France uses interrupt 1 and interrupt 3, with a variable key sequence.

This means that you cannot single step through the virus. Every so often in the ***V2*** series there is a 0cch instruction in the virus, which calls interrupt 3 and interrupt 1 to decrypt the next two bytes using one as the key and the other as the byte to decrypt. But you cannot write a program to automatically do the decryption, because there are also dummy 0cch bytes that do not get executed, and thus do not decrypt the following bytes. So if you write a program to treat each 0cch byte that way, you will scramble those parts of the program, as well as decrypting the parts that need decrypting. The virus author has posed yet more problems. To scan for the virus, you must understand the code generator, and to do that you have to disassemble the virus, which means that you have to break through the confusion. It is all possible, but it all takes time.

When a Dr Solomon's researcher disassembled ***Fish6***, he said that it took two weeks to do the virus, and another two weeks to uncross his eyes. Disassembling ***Whale*** is similar to doing a very difficult crossword puzzle. If you ever get cast away on a desert island with a PC and Debug, and you get to choose one virus to take with you for entertainment, make it ***Whale***. Even a year after it first came out, the majority of scanner products were not able to detect all the faces that it could present to the world. This makes ***Whale*** quite a good test of the research and development in the field.

Fortunately, ***Whale*** is incapable of working in a real environment, but there is always the possibility of Son of Whale. The technique of extreme confusion is sometimes called 'armouring', but it is a very standard thing in the copy protection field, where the copy protection vendors are keen that would-be pirates should not be able to understand their code.

Having discussed the theory of stealth, it is now possible to discuss a real example, and the impact of it. The ***Tequila*** virus is quite common in Europe, and has been seen in the US. It was written in Switzerland and planted on the distribution disks of a shareware vendor by a friend of the author. This gave it a good start in life.

When you run an infected EXE program, ***Tequila*** installs itself on the partition sector of the hard disk. To do this, it uses another stealth technique called 'tunnelling'. In the case of ***Tequila***, it puts the processor into single-step mode, and calls interrupt 13h to reset the disk. But on every instruction, interrupt 1 is called, and ***Tequila*** has reprogrammed the interrupt to look at the location in memory from which it is being

 Copyright © Dr Solomon's Software

called. When ***Tequila*** finds that the interrupt is being called from the firmware, it stores that address, and switches off the single-step mode. Now ***Tequila*** knows the address of the hard disk controller firmware. Any program that is supposed to be blocking attempts to write to the hard disk via the interrupts is very easily evaded by doing a far call to the firmware. Then ***Tequila*** installs itself on the partition sector.

The next time that the computer is booted, the partition sector is run, and this happens before any anti-virus software can be run. The virus is installed into memory, and ***Tequila*** then stealths the partition sector so that any anti-virus software examining the sector sees what was there before ***Tequila***.

Now ***Tequila*** can start infecting files. It has a complex code generator in the body of the virus, so that the decryptor/loader of the rest of the code is very variable. There are a few 2-byte strings for which you can scan, and some 1-byte strings that are reliably there. But some scanners have difficulty detecting all instances of the virus, and some scanners give false alarms on otherwise innocent files because of the difficulty in doing it right.

The virus adds 2468 bytes to each infected file. But with the virus in memory, the growth in file size is concealed from programs that ask DOS for this information. So the virus is quite difficult to see, and easily gets copied onto disks and passed on.

The main outcome of the virus is a kind of Mandlebrot fractal display in block graphics, three months after installing the virus on the hard disk. The main way that users notice the virus is when some program is incompatible with the virus, for example, Windows.

The general solution to the polymorphic virus problem

As the polymorphic engines got more and more complex, it gradually became clear that writing algorithms to detect each one was not the way to go. The Dark Avenger's Mutation Engine was about three days work for most of the top Anti-Virus researchers, and if something like that appears a few times per month, then it is hard to keep up. So at Dr Solomon's, we looked for a more generic solution, one that wouldn't involve writing code for each new virus.

The answer was generic decryption. A generic decryptor looks at the virus, and works out what bytes would appear if the body of the viruses were to be decrypted. Then, with those bytes in a buffer, it is very simple to do a simple signature scan to detect the virus in the old way, and it's also possible to do an exact identification of the virus by checksumming the decrypted bytes, and then repair. We wrote the

Copyright © Dr Solomon's Software

Generic Decryption Engine (GDE) in 1993, and the first virus we tried it on was "ITSHARD", which used the Nuke Encryption Device (NED). An estimate of the amount of R&D needed to get reliable detection for this virus, using the old algorithmic methods, came to about ten man-days. Using the GDE, it took half an hour.

Generic decryption also eliminates false alarms. If you use a complex algorithm to look at the relationships between the bytes in the decryptor, you could easily mistake an innocent file for one that vaguely resembled the virus (and even in 1996, some products give that kind of false alarm). But if you can calculate what the encrypted bytes would look like if they were decrypted, then you can do a straightforward signature match, and either you get a match between the 20 bytes you're looking for, or else you don't.

But the main benefit of the GDE, is that it gives the antivirus company a way to respond quickly to new polymorphic viruses, without having to go through the lengthy process of program development and testing, by just adding a description of that virus to the database. By mid 1996, a few Anti-Virus companies had implemented generic decryption, and most of the others were looking at doing so.

The future

Most of the viruses that are seen are noise viruses, that is, yet another version of ***Vienna, Burger*** or ***Jerusalem***. But some of the virus authors are writing viruses that are designed to be difficult to detect, and survival of the fittest will of course ensure that these are the viruses that are most likely to become common in the long term. When all users are running the kind of simple scanner that can detect ***Jerusalem*** and ***Stoned***, the only viruses that will spread will be the ones that make good use of polymorphism techniques.

Polymorphism, therefore, will be increasingly important in the future. The consequence is that more and more viruses will be difficult to deal with from the point of view of the virus researcher. From the point of view of the user, there will be more and more false alarms as scanners mistake innocent files for some of the results of the sophisticated code generators. Also, there will be an increasing number of situations where the scanner in use is not capable of detecting the virus; not because the scanner has not yet been upgraded to deal with a new virus, but because it is simply too much work for the vendor to keep up with the flood of new, and difficult viruses.

 Copyright © Dr Solomon's Software

7. PC Viruses

The Virus naming problem

When anti-virus researchers find a new virus, they want to upgrade their software to detect it right away. But when the software finds the virus, a researcher has to call it something. What name should it be given?

Whatever the researcher decides to call it, they can be quite sure that three other anti-virus researchers are working on the same virus at the same time as them, and that they are each also giving it a name, and very often none of them are picking the same name. Viruses seldom come with a name conveniently attached. A few do have an obvious name enclosed in the virus by the virus author, but there is some reluctance to use such a name even in the few cases where it exists, because it tends to encourage and gratify the author. Still, whenever there is any text in a virus, it is likely that part of it will become the virus's name. This is how ***Stoned*** virus also came to be known as ***Marijuana***, since both words are in the virus. Other researchers named ***Stoned*** for the geographical location in which they believed it had first been found. Hence it is also known as ***New Zealand, Australian, Hawaii, San Diego***, and ***Smithsonian***. This is clearly not a good way to name viruses, and has the further problem that other completely unrelated viruses may be discovered in the same places. A further convention names viruses for the length they add to a file when they infect. This is no use for boot sector viruses like ***Stoned***, and leads to confusion with viruses whose length varies or which have the same length as each other. When there is a characteristic infective length, it can be useful for distinguishing variants of a single virus. Viruses have been named for the dates when their payload triggers, leading to a certain amount of competition for popular days, with several completely different viruses being known as ***Friday the 13th***. The well-known ***Michelangelo*** virus is actually named for a date. There is nothing in the virus that refers to ***Michelangelo*** at all, but it triggers on March 6th, which is Michelangelo's birthday. Viruses can also be named for their payload, for example, ***Ping-Pong*** and ***Cascade***, named for the screen effect they produce, and ***Yankee Doodle***, named for a tune it plays. Unfortunately there are other viruses that borrow these effects, and sometimes are given confusingly similar names.

People who use more than one anti-virus product are often disturbed to find that they do not agree about the name of a virus. Sometimes they think that one product does not find the viruses that the other product finds, because it does not document them by the same names. The only way this confusion can be resolved is for

Copyright © Dr Solomon's Software

everyone to realize that there is NO CORRECT NAME for any virus. Dr Solomon's uses the system that it uses for a number of reasons that make sense. For one thing, it is the EICAR, the European Institute for Computer Antivirus Research, approved convention as used by several anti-virus products. Other people use other systems that they prefer, each system tending to be used by a single product.

There is a naming standard, but it is mostly to do with what you cannot use as a name (someone's brand name, a company name, a living person's name, a geographical area 'where it was first found'). This standard is available from the University of Hamburg, together with a document giving the agreed Computer Anti-Virus Research Organization (CARO) names for almost all existing viruses.

In this book, Dr Solomon's lists its preferred name first, and any other names it is aware of as aliases. Occasionally, Dr Solomon's changes its mind about a name (usually because an international naming agreement has been reached for that virus), or even re-arranges part of the system of classification. So do not be too surprised if the names in this book do not always match the names reported by the on-line Virus Encyclopedia in Dr Solomon's Anti-Virus Toolkit.

Additional information

Additional information about these viruses, and about viruses not covered in the printed documentation, is available in the on-line Virus Encyclopedia in Dr. Solomon's Anti-Virus Toolkit or on the Dr Solomon's web site (www.drsolomon.com).

The viruses

The Virus Encyclopedia is arranged as descriptions in the following format:

Common Names (Aliases)

Common names are ***bold, italic*** when mentioned in the text.

Type

Boot sector, partition sector, file, macro, other.

 Copyright © Dr Solomon's Software

Boot sector viruses infect the boot sectors of floppy disks, and either the boot sector or the partition sector of hard disks.

Partition sector viruses are very similar to the boot sector viruses in that they infect the boot sectors of floppy disks, and the partition sector of hard disks.

File viruses infect files. This may be just COM files, just EXE files, or both.

Some viruses go memory resident. These are the ones that you are most likely to come across, as non-memory resident viruses are not sufficiently good at copying themselves to spread well.

Multipartite viruses are both boot and file viruses.

Companion viruses create a COM file where previously there was only an EXE file. DOS runs the COM file in preference to an EXE file with the same name.

Overwriting viruses overwrite the code at the start of the file with their own code – the original program then does not work. As a result, such viruses are so poor at spreading that you are highly unlikely to ever see one.

Macro viruses infect certain types of document or spreadsheet files, by linking macros containing virus code to a document or spreadsheet. Potentially, macro viruses could be written for any macro writing language which is sufficiently powerful. To date (October, 1996) we have seen macro viruses for Microsoft Word for Windows, Microsoft Excel for Windows and Lotus AmiPro.

See Chapter 1, "About Viruses", for more detailed information.

Affects

Types of files infected.

File Growth

Amount by which files grow.

Viruses add their code to the infected file. Boot and partition viruses, of course, do not, and neither do overwriting or companion viruses. The File Growth entry tells you by how much to expect to see a file grow. This value can be different for different files – some viruses round up the file size before infecting it, others deliberately have a variable size.

Description

What it does and the effects.

Variants

What variants there are and their effects.

Copyright © Dr Solomon's Software

Dr Solomon's uses the common name for the virus that has been standardized by EICAR, the European Institute for Computer Antivirus Research, and by CARO, the Computer Antivirus Research Organization.

Dr Solomon's also give some of the names (aliases) used by other products to refer to the virus. Unfortunately this list cannot be comprehensive.

Variants are in **bold** when mentioned in the text.

3APA3A (Zaraza)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The name of the virus, *3APA3A*, in Russian slang means 'infection'. The alias, Zaraza, is the Russian pronunciation of *3APA3A*.

3APA3A uses a complex infection method. It infects boot sectors of floppy disks in a similar manner to other boot sector viruses. However, on hard disks, the virus infects the DOS kernel file IO.SYS.

The size of the virus is 1,024 bytes (that is, two sectors). On floppy disks, the first part of the virus is stored in the boot sector. The second part of the virus and the original floppy disk boot sector are stored at the end of the disk's root directory. Thus when the virus infects a disk, it also overwrites the last two sectors in the root directory.

When a PC is booted from an infected disk, the virus tries to infect the first file (usually IO.SYS) in the root directory of the active DOS partition. The virus begins by making a copy of the IO.SYS file, after which it infects the original file. After the infection, the root directory contains two IO.SYS entries. However, because the virus sets the volume-label bit, the first IO.SYS entry is not shown in a directory listing. The directory entries point to the two IO.SYS files. The first directory entry points to the first IO.SYS file, which is located in its usual place at the start of the root directory. Except for the virus code at the start, this file is unchanged. The second directory

 Copyright © Dr Solomon's Software

entry points to the copy of the original IO.SYS file, which is located at the end of the partition. This copy is not infected.

When DOS is started during the next boot-up, the infected IO.SYS is executed and the virus loads itself into memory. Then it infects all non-write-protected disks that are used in the PC.

Infected hard disks carry the label 'IO.SYS'. The label can be seen with the DIR and LABEL command, but the label cannot be changed even with the LABEL command.

3APA3A is mildly polymorphic – the boot sectors of infected disks vary slightly. Only the string **MSDOS 5.0** can be seen at the beginning and the 55AA marker is present at the end of the boot sector.

The virus contains the message **B BOOT CEKTOPE 3APA3A!** (which means, **IN BOOT SECTOR – INFECTION!**). The message string is encrypted and cannot be seen even in memory. In August, the virus displays its message during every PC boot-up.

3APA3A does not contain destructive routines.

Because of a bug, the virus frequently hangs 386/486 computers. *3APA3A* can only infect hard disks whose active DOS partition sector is bigger than 10.6 Mb.

10 Past 3

Type

Memory resident file virus.

Affects

COM files on execution. Only files between 4 and 64,496 bytes are infected.

File Growth

748 bytes.

Description

On the 22nd of each month, the PC re-boots. On various dates, various peripherals are disabled or made unreliable:

1st	Keyboard
10th	Hard disk
16th	Monitor
29th	Disks

Copyright © Dr Solomon's Software

Between 15:10 and 15:13 each day, a keyboard trick is installed which causes the **Ctrl** or **Shift** key to be invoked, each with a 4.5% probability, on each keystroke.

Ahav

Type
File virus.

Affects
COM files in the current directory, each time an infected program is run.

File Growth
-

Description
The virus is a primitive, encrypted, non-resident infector, 377 bytes long. The virus contains (beneath the encryption) the text:

```
[AHav] Gothmog/DHA
```

and

*.COM

where DHA stands for 'Digital Hackers' Alliance'.

This virus was initially posted by its author to an internet newsgroup.

Aids (Number 1)

Type
Overwriting file virus.

Affects
A COM file in the current sub-directory on execution of an infected file.

File Growth
Files are overwritten and grow to 13,952 bytes if they are less than that.

Description
The original program no longer works. With color screens the system hangs.

This virus has nothing to do with the Aids Information disk, a trojan which was mailed to several thousand users in December 1989.

Copyright © Dr Solomon's Software

Aircop

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
The original boot sector is written to cylinder 39, head 1, sector 9.
The virus displays the message:

```
RED STATE, Germ offensing --AIRCOP.
```

Variants
Aircot, AircopNGa, b and **c, Standard**.

Akuku

Type
File virus.

Affects
COM and EXE files when an infected COM file is run. Only files between 1,000 and 64,000 bytes are infected.

File Growth
COM: padded out to a multiple of 16 bytes, then 889 bytes are added.
EXE: padded out to a multiple of 16 bytes, then 892 bytes are added.

Description
At between 20 minutes and 23 minutes past each hour, if an infected program is run the message **`A kuku, Nestepny komornik !!!`** is displayed.

Variants
b:
As above, but displays the message
`(C) by Metal Thunder IVRL MI.`
`Copmpletely:`

This says **`Sorry, I'm copmpletly dead..`**

Copyright © Dr Solomon's Software

c:
One byte has been replaced with CCh, the 1-byte interrupt. This was probably done accidentally by a virus researcher.

Alabama

Type
Memory resident file virus.

Affects
EXE files on execution.

File Growth
1,560 bytes.

Description
Whenever a COM or EXE file is loaded, the next uninfected EXE file in the current sub-directory is infected. Read-only files are set to R/W, then reset after infection.

When the hour changes, the message **`SOFTWARE COPIES ARE PROHIBITED BY INTERNATIONAL LAW xxxxx 00000012 xxxxxxxxxxx Box 1055 Tuscambia ALABAMA USA`** is triggered and the PC hangs. On a color monitor the message is red and surrounded by a red blinking double-line box.

Any file starting with DEBU or SYMD will not be infected but is modified to become unusable. This is aimed at DEBUG and SYMDEB. If the virus is in memory, the DOS COPY command and many other file-opening operations don't work properly. The virus will survive a warm boot (Ctrl Alt Del) and will continue to infect other programs afterwards.

Variants
a and **b**.

Alfons

Type
Memory resident file virus.

Affects
COM and EXE files.

Copyright © Dr Solomon's Software

File Growth

See Variants.

Description

This virus uses a prepending method of infection for COM files; and an appending method of infection for EXE files.

The virus is not encrypted.

Both variants use INT_3 as an internal replacement of DOS INT_21h. The only intercepted functions are 4B00h (load and execute file) and 4Ch (exit).

Variant **1344** (which is actually an improved variant of **1536**) uses 32-bit instructions.

For self-recognition of infected files, the virus uses 2 bytes at the very end of the file. For the **1344** variant, they are 50 7D (P}); for the **1536** variant, they are 50 7B (P{).

No strings are visible in the virus.

Variants

1344, 1536.

Ambulance (Redx, Red Cross)

Type

File virus.

Affects

Two COM files in the current sub-directory or path, on execution of an infected file.

File Growth

796 bytes.

Description

When an infected file is executed, the virus looks for two COM files to infect, first in the current directory and then down the path.

Every eighth (starting with the sixth) time an infected application is run, the ambulance is triggered. This is a small car which travels across the bottom of the screen with the two-tone siren of a German ambulance.

Variants

One variant triggers the ambulance every time an infected file is run. There is also another minor variant.

Copyright © Dr Solomon's Software

Amoeba (1392, Khetapunk)

Type
Memory resident file virus.

Affects
COM and EXE files on execution. COM files smaller than 512 bytes and larger than 60Kb bytes are not infected.

Date/time and read/write/hidden attributes are not preserved.

File Growth
1,392 to 1,407 bytes.

Description
The virus contains **`KHETAPUNK - NOUVEL Band A.M.O.E.B.A. by PrimeSoft Inc`** in encrypted form. The virus takes up 3Kb of memory when resident.

There are no noticeable effects because of bugs in the code.

Angelina (Stoned.Angelina)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
This stealth boot sector virus infects hard disks when booted from an infected floppy disk. Disks are infected on read and write access (for example, the DIR or COPY commands).

Functionally, the virus is similar to *Stoned*. On hard disks the original partition sector is re-located to cylinder 0, head 0, sector 9.

The virus contains the following encrypted text, which is never displayed:

`Greetings for ANGELINA !!!/by Garfield/Zielona Gora`

Variants
There are two slightly different variants of the virus.

 Copyright © Dr Solomon's Software

Anthrax

Type
Multipartite.

Affects
COM and EXE files on execution of an infected file, and the partition sector.

File Growth
1,024 to 1,280 bytes.

Description
When an infected file is executed, another file is infected.

The text **`(c) Damage, Inc.`** is in the file, indicating a Bulgarian origin, as is the word **`ANTHRAX`**. Some PCs will not boot with *Anthrax* in the partition sector.

Anticad (Taiwan 3, Taiwan 4, Plastique, Invader, Hammer)

Type
Memory resident file virus.Versions 1 and 4 (see below) are also boot sector viruses.

Affects
COM and EXE files on execution or copying.

File Growth
Anticad 1 4,096 to 4,111 bytes.

Anticad 2 2,900 to 2,915 bytes.

Anticad 3 3,004 to 3,019 bytes.

Anticad 4 4,096 to 4,111 bytes.

Anticad 5 2,576 to 3,103 bytes.

Description
If a program called ACAD is run, the trojan triggers. It disables the keyboard, clears the screen, overwrites drive A (head 0 and all tracks), then does the same to drive B. Next it overwrites drives C and D cylinder 0, all heads, and works down the disk incrementing each track by an amount which itself increments for each step. Finally, it overwrites CMOS with 0FFh and hangs the system.

A less vicious variant is triggered 2,000 keystrokes after the last write, and disables hard disk-writes.

A third trick is to play music after a delay. There are three variants:

Copyright © Dr Solomon's Software

Blue Danube
Classical tune
Chinese tune

This virus looks as if it has been influenced by *Jerusalem*.

Anticad 5 does not contain the destructive routine, but plays music. This variant may predate *Anticad 2* which was previously thought to be the earliest. *Anticad 5* contains the following string:

```
To Whom see this: Shit! As you can see this document, you may
know what this program is. But I must tell you: DO NOT TRY to
WRITE ANY ANTI-PROGRAM to THIS VIRUS. This is a test-program,
the real dangerous code will implement on November. I use MASM
to generate various virus easily and you must use DEBUG against
my virus hardly, that is foolish. Save your time until next
month. OK? Your Sincerely, ABT Group., Oct 13th, 1989 at FCU.
```

AntiCMOS (Lenart, LiXi)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus infects the hard disk when booted from an infected floppy disk. Disks are infected on read or write access (for example, DIR or COPY commands).

When infecting, the virus does not save the original boot and/or partition sector, but patches itself into the original.

Variants

AntiCMOS.a and **b**.

Variant .a:

The virus does not corrupt CMOS. Instead the computer emits a periodic sound and hangs. The virus contains the message **I am Li Xibin!**.

 Copyright © Dr Solomon's Software

Variant .b:
On floppy disk access, there is an approximate 1-in-256 chance that the virus will trigger, and then erase CMOS data by writing to the fields containing floppy and hard drive types (CMOS bytes 10h and 12h). The hard disk C becomes 'Not installed'. The floppy drive A is changed as follows:

If it was 5.25" 360Kb it becomes 3.5" 720Kb

If it was 5.25" 1.2Mb it becomes 'not installed'

If it was 3.5" 720Kb it becomes 5.25" 360Kb

If it was 3.5" 1.44Mb it becomes 5.25" 1.2Mb

If it was 'Not installed' it becomes 5.25" 1.2Mb

Since the virus does not re-calculate the CMOS checksum, the BIOS should display the CMOS CHECKSUM FAILURE error message on the next re-boot.

The virus has no specific strings inside.

AntiEXE (D3, NewBug, CMOS4)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
This virus infects the hard disk when booted from an infected floppy disk. Disks are infected on read access (for example, DIR or COPY commands).

When a certain (unknown as yet) EXE file is being executed or read from a disk (for example, using the COPY command) the virus patches the first byte of the in-memory file image, thus causing unpredictable errors. In most cases the PC hangs.

Variants
There are two slightly different variants, including **AntiEXE.a**.

Copyright © Dr Solomon's Software

Anti-Pascal (AP-400, AP-440, AP-480, AP-529, AP-605)

Type
File virus.

Affects
A COM files between 2Kb and 64,000 bytes (but may vary: see below) on execution of an infected file.

File Growth
Bytes as indicated by the variant name.

Description
When an infected file is executed, the virus scans through the drives for another COM file to infect.

Variants
AP-400:
When there are no more files to infect, it deletes any files with the extension ?A?.

AP-440:
When there are no more files to infect, it deletes any files with the extension P?? or BAK.

AP-480:
When there are no more files to infect, it deletes any files with the extension P?? or BAK. It also overwrites the directory entries by creating then deleting temporary files.

AP-529:
Affects files between 529 and 65,506 bytes. When it cannot find any more files to infect, it deletes all BAK files and renames all PAS and EXE files to COM before deleting them.

AP-605:
Affects files between 605 and 64,930 bytes. When it cannot find any more files to infect, it overwrites PAS files with itself and then renames them to COM files.

Arab

Type
Memory resident file virus.

Affects
COM files on execution. Files must be greater than 27 and less than 64,445 bytes.

 Copyright © Dr Solomon's Software

File Growth
834 bytes.

Description
The text **`nsed Materi`** can be found in the virus.

After an infected file has been run 256 times, the virus patches the partition sector to make the hard disk non-bootable.

ARARA

Type
File virus.

Affects
A COM file in the current sub-directory on execution of an infected file.

File Growth
Variable: 1,052 to 1,067 bytes.

Description
This non-resident virus is variable encrypted and polymorphic.

As the virus uses 80286-specific instructions, it will not operate properly on pre-80286 PCs (most XTs).

The virus has no payload. It contains the encrypted strings **`[ARARA], *.OCM`** and the following text:

`ILASA MICALAZODA OLAPIRETA IALPEREJI BELIORE: DAS ODO BUSADIRE OIAD OUOARESA CAOSAGO: CASAREMEJI LAIADA ERANU BERINUTASA CAFAFAME DA IVEMEDA AQOSO ADOHO MOZ, OD MAOFASA. BOLAPE COMO BELIORETA PAMEBETA. ZODACARE OD ZODAMERANU! ODO CICALE QAA. ZODOREJE, LAPE ZODOREJE, LAPE ZODIREDO NOCO MADA, HOATHAHE SAITAN!`

Arianna

Type
Boot sector virus.

Copyright © Dr Solomon's Software

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
The virus has a memory resident payload and infection system. It has advanced stealth capability. The whole virus is encrypted. It displays a message.

Variants
3375 and 3426.

Armagedon (The Greek)

Type
Memory resident file virus.

Affects
COM files on execution, except COMMAND.COM and files with ND as the sixth and seventh letters. Only files between 1,079 and 57,344 bytes are infected.

File Growth
1,079 bytes.

Description
The text **`Armagedon the GREEK`** is contained in the virus.

Between 5 a.m. and 6 a.m., the virus sends **`+++aTh0m0s7=35dp081,,,,141`** to the comms port. This has the effect of hanging up then dialling 081 141.

AT144

Type
Memory resident file virus.

Affects
COM files on execution. Only works on PCs with 286 processors and above.

File Growth
144 bytes.

 Copyright © Dr Solomon's Software

Description
There is no payload.

Variants
There is a corrupted version which does not work. There are also 132-byte and 149-byte versions.

Attention

Type
Memory resident file virus.

Affects
COM files on execution. Only files between 786 and 64,921 bytes are infected.

File Growth
394 bytes.

Description
The text string **`ATTENTION!`** will be found near the start of infected files. The Critical Error Handler giving the DOS message **`Write protect error writing drive X: Abort, Retry, Ignore?`** is permanently disabled.

Avispa.2048

Type
Memory resident file virus.

Affects
EXE files.

File Growth
-

Description
This is a polymorphic virus.

The virus intercepts INT_13 and INT_21. It checks for itself in memory by issuing a call, AX=4BFF/INT_21h; the correct response is AX=4BFE.

The virus avoids infecting files *AN.*, *LD.*, *OT.* and files where CS:IP=0:0 (apparently to avoid some AV programs like SCAN and simple 'sacrificial goat' files).

Avispa.2048.d (the most common variant) contains the following

Copyright © Dr Solomon's Software

strings:

```
__ Virus Avispa - Buenos Aires - Noviembre 1993 __
$$ Virus AVISPA $$ Republica Argentina$$ Elijah Baley
$$ Noviembre 10 de 1993
$$ This program is not an old virus variant, and it was
written in Argentina by Elijah Baley. It uses polymorphic
technics to avoid conventional scanning.
$$ MENEM: Libertador de torturadores y asesinos de inocentes,
que Dios se apiade de tu pobre alma. $$.
```

Variants

2048.a-f.

BackFont (V905, Topsy-905, Backfont-905)

Type

Memory resident file virus.

Affects

EXE files on execution.

File Growth

900 to 905 bytes.

Description

Twenty seconds after infection, the screen fonts on EGA and VGA monitors are reversed.

Some variants trash the hard disk.

Backtime

Type

Memory resident file virus.

Affects

COM files on execution, if less than 6,000 bytes long.

Copyright © Dr Solomon's Software

File Growth
528 bytes.

Description
The text string **Backtime** can be found in the virus, and the system clock appears to run backwards.

Variants
Prague Blinker:
Files grow by 512 bytes. A blinker effect happens about once every 15 seconds.

Prague Joker:
Files grow by 496 bytes. On each timer tick (18.2 times per second) there is a 1-in-256 chance that the stack will be slightly corrupted. This leads to problems in running programs, and system crashes.

Prague Shaker:
Files grow by 152 bytes. The monitor seems to lose vertical synchronization about once a second. This looks like a hardware problem.

Bad Boy

Type
Memory resident file virus.

Affects
COM files on execution.

File Growth
1,001 bytes.

Description
The virus is encrypted.

It avoids being noticed by generic active monitors by using various techniques to get past traps for interrupt 13h.

Variants
Bad Boy.a:
This contains the encrypted text **The bad boy halt your system...** and **The Bad Boy virus, Copyright(C) 1991.**

Bad Boy.b:
This contains the encrypted text **Make me better!** and **The Bad Boy virus, version 2.0, Copyright(C) 1991.**

Copyright © Dr Solomon's Software

Bad Guy

Type

Overwriting file virus.

Affects

COM files in the current sub-directory when an infected program is run.

File Growth

None, but the first 264 bytes are overwritten.

Description

Because of the overwrite, infected programs no longer behave as expected. There is a text string in the virus which is:

```
BadGuy virus (c) by Cracker Jack 1991 (IVRL) Italian Virus
Research Laboratory (C) 1990, 1991 IVRL Head Quarter, Milan
Italy.
```

On Mondays, the virus re-programs the video controller for CGA monitors so that the horizontal trace is out of synchronization and the picture breaks up.

Badsec

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

Description

Badsec is not in the wild, but it could be in the future.

It is quite infectious and results in minor damage.

The virus has a memory resident payload and infection system. It has minimum stealth capability. This virus is not encrypted. There are no other effects.

Variants

3422 and 3428.

Copyright © Dr Solomon's Software

Bandit

Type
Memory resident, file virus.

Affects
EXE files when an infected program is run.

File Growth
1,641 bytes.

Description
The string **!!PCBANDIT!!** can be found at the end of infected files.

On Mondays the virus re-formats the third floppy disk drive, device 2. This was probably meant to be the hard disk.

Barrotes

Type
Memory resident file virus.

Affects
COM and EXE files (except variant 849, which infects COM files only).

File Growth
See Variants.

Description
The virus is not encrypted (except **Barrotes.1303**). *Barrotes* always tries to infect COMMAND.COM (all variants contain the string **COMMAND.COM**). When infecting EXE files, the virus does not modify the current SS:SP, which means that some infected files will be corrupted.

To detect itself in memory, the virus issues the call AH=EE/INT_21; the correct response is AL=FE (**Barrotes.1127** uses AX=AAAA/INT_21 -> AX=BBBB; **Barrotes.1463** uses AX=EEFF/INT_21 -> AX=FFEE;

Barrotes.1874 uses AH=EC/INT_21 -> AL=EF).

On the 5th of January, **Barrotes.849** overwrites the partition sector and prints:

Virus BARROTES por OSoft

This message appears on a background of vertical colored lines.

Copyright © Dr Solomon's Software

Variants

849, 1127, 1194, 1303, 1310, 1463, 1874.

The following strings and payloads are present in other virus variants:

1127 uses SO (53 4F) as a marker at the end of the file for self-recognition. It has no payload.

1194 has a bug in the payload which prevents it from overwriting the hard drive on the 1st of each month, as intended.

1303 displays **`sta Tecla (MAD1)`** and changes the codes of keys being pressed on 23 September.

1310 displays **`Virus MIKELON por MSoft`**. It overwrites the partition sector on 5 January (one minor sub-variant does not have this destructive payload).

1463 overwrites the partition sector on 22nd of any month.

Batman

Type

File virus.

Affects

COM files.

File Growth

-

Description

Infection of a hard disk begins with the introduction of a batch file, for example, INF.BAT. This would look something like:

```
@echo off
rem<machine code instructions interpreted as ASCII>
copy INF.BAT INF.COM > nul
INF
del INF.COM
```

In other words, when the batch file runs, it is renamed to a COM file. Then the virus instructions are executed (and the virus does whatever the author chooses to include), after which the COM file is deleted.

Copyright © Dr Solomon's Software

Bebe

Type
File virus.

Affects
A COM file (unless set to read-only) on execution of an infected file.

File Growth
Padded to a multiple of 16 bytes, then 1,004 bytes are added.

Description
The text strings **`VIRUS1, Skagi bebe`** and **`Fig Tebe!`** can be found in the virus. If it cannot find another file to infect, ten minutes after it has finished trying, it pops up a window in the center of the screen containing:

```
VIRUS!
Skagi bebe
```

However, the PC hangs when it tries to install the interrupt to enable this display.

Beijing (BuptBoot, WelcomB, Bupt 9146)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
The virus does NOT store a copy of the original, clean partition sector elsewhere on the disk. It stores additional virus code on cylinder 0, head 0, sector 4 on the hard disk and in one of the root directory sectors on floppy disks. The text **`Welcome to BUPT 9146, Beijing!`** can be found in this sector.

Best Wishes

Type
Memory resident file virus.

Copyright © Dr Solomon's Software

Affects
COM and EXE files on execution. COM files of less than 512 bytes and greater than 60,000 bytes are not infected.

File Growth
1,024 bytes.

Description
At the end of the virus is the text string **`This program ..With Best Wishes!.`** Any infected program run on Friday 13th will first display the message **`With Best Wishes!`**. When you exit the program the message is displayed repeatedly. At the same time the boot sector is patched so that DOS thinks the disk has 0 sectors. On other days it reduces the count of the number of sectors by one cluster plus 256 sectors.

Variants
There are two, one of which causes file growth of 970 bytes and the other, which fails to infect EXE files.

BestWishes 1:

This does not use the INT2Fh tunnel to evade interrupt blockers, and the text message is **`With Best Wishes.`**

Better World (Fellowship)

Type
Memory resident file virus.

Affects
EXE files on execution. The file date and time are not preserved after infection.

File Growth
1,019 to 1,034 bytes.

Description
The following text string can be found:

`This message is dedicated to all fellow PC users on Earth`
`Towards A Better Tomorrow And A Better Place To Live In`

The string **`03/03/90 KV KL MAL`** may also be found (see *Black Monday*). If the virus goes memory resident during September, the message is displayed in 320x200 graphics mode each time a program is run.

This virus is another derivative of *Jerusalem*, and a close relative of *Black Monday*.

Copyright © Dr Solomon's Software

Big Joke

Type
File virus.

Affects
A COM file when an infected file is run. COMMAND.COM is not infected.

File Growth
1,068 bytes.

Description
If the system clock seconds counter stands at between 0 and 4 seconds when the virus is run, the following messages are displayed:

```
At last.......ALIVE!!!!!
I guess your PC is infected by the Big Joke Virus.
Release 4/4-91
Lucky you, this is the kind version.
Be more careful while duplicating in the future.
The Big Joke Virus, killer version, will strike harder.
The Big Joke rules forever.
```

Each message is displayed in the center of the screen, and is faded in and out by cycling through shades of blue.

Blackjec (Bljec)

Type
File virus.

Affects
COM files in the current directory when an infected file is run. In most versions the date is set to the current date.

File Growth
Variable, depending on the variant.

Description
There is no payload.

Variants
Blackjec 3:
Files grow by 231 bytes.

Copyright © Dr Solomon's Software

Blackjec 4:
Files grow by 247 bytes. Files, which would increase the 64Kb COM file limit if infected, are ignored.

Blackjec 5:
Files grow by 267 bytes, and files containing the string **MZ** are not infected as they may be EXE files.

Blackjec 6:
As **Blackjec 5**, but files grow by 276 bytes. Files conforming to CO*.COM are avoided.

Blackjec 7:
As **Blackjec 6** but files grow by 287 bytes and only three files are infected on each run.

Blackjec 8:

As **Blackjec 7** but files grow by 358 bytes and the date is preserved.

Blackjec 9:

As **Blackjec 8** but files grow by 369 bytes and the check for **MZ** is different.

There are also **b** versions of the listed variants.

Black Monday

Type
Memory resident file virus.

Affects
COM and EXE files on execution.

File Growth
1,055 bytes (EXE files may vary).

Description
The text string **Black Monday 2/3/90 KV KL MAL** can be found in the virus (see *Better World*). When the virus is run on a Monday the trojan is enabled. A counter counts down from 240 each time a file is infected, and when it reaches 0 a low-level format is done of head 1 on the hard disk, starting at cylinder 1 and stepping inwards.

This virus appears to be a re-write of *Jerusalem*.

 Copyright © Dr Solomon's Software

Blood

Type
File virus.

Affects
A COM file of less than 32Kb on execution of the infected program.

File Growth
418 bytes.

Description
There is a 1-in-8 chance that the message **`File infected by BLOOD VIRUS version 1.20`** will be displayed. This is visible in the virus.

Boot-437 (bath, Square)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
This is a very simple boot sector virus. It infects both 720Kb and 1.44Mb floppy disks. It uses 1Kb of RAM.

It intercepts the read and write functions of INT_13.

To check if a sector is already infected, the virus compares 6 bytes at offset 100h (they must be 05 0e 1f e8 08 00).

Boot droppers

These are not viruses themselves, but drop a virus when run, the dropper program warns you that they are about to install a virus on drive A.

Copyright © Dr Solomon's Software

BootEXE.451 (BFD-451)

Type
Multipartite virus.

Affects
Floppy and hard disks, and EXE files.
The virus takes 4Kb of DOS RAM (see Description).

File Growth
-

Description
The virus is a 'fast infector'. It does not stealth the original DOS boot sector or EXE file contents. The original boot sector is re-located to cylinder 0, head 0, sector 11.

The virus takes 4Kb of DOS RAM. This is visible using CHKDSK and MEM.

For EXE files (starting with the **MZ** signature) of less than 64Kb, the virus infects the EXE header if there is enough free space after the relocation table. The virus converts an EXE file into a COM file.

Self-recognition in memory is INT_13 with AH=F0. The correct response is AH=19h.

Infected files can re-infect the system if just the boot sector is cleaned.

When the virus is memory resident all suitable EXE files accessed in any way (read, write, execute) are infected.

The virus has no strings inside. It has no payload.

Variants
394, 396, 443, 451, 452.

Bosnia (TPE_Bos)

Type
Virus.

Affects
COM and EXE files.

File Growth
Approximately 3Kb.

Copyright © Dr Solomon's Software

Description

The virus is not memory resident. It has no stealth capability and is very visible. The virus is not encrypted. There are no other effects.

Variants

Adin, Girafe.a-d, Nondes, Poetcode, Eccles, Youba.

Boys-500

Type

File virus.

Affects

COM files when an infected file is run.

File Growth

500 bytes.

Description

The virus contains the string **`The good and the bad boy.`**

COM files are made read-only and EXE files have the system attribute set.

Boza

Type

File virus.

Affects

EXE files in Windows 95 executable file format.

File Growth

3Kb.

Description

Boza is extremely unexceptional and unsophisticated. It is a direct action (non-resident), appending virus.

Boza comes from Australia and infects program files which are in Microsoft's Windows 32 Portable Executable (PE) file format. This means that it can infect Windows 95 and Windows 32S executable files.

Copyright © Dr Solomon's Software

Boza infects up to three files in the current directory whenever an already infected program is run. It does not go resident in memory which seriously reduces its ability to spread and thus get into the wild.

Boza does not carry a destructive payload - its sole purpose seems to be an attempt to spread. Even this it fails to do successfully, sometimes ruining files that it attempts to infect. The virus displays a dialog box on the 31st of the month.

Brain (Pakistani, Pakistani Brain, Lahore, Ashar, UIUC)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The volume label of the infected floppy disks is changed to **(c) Brain** and infected disks have 3Kb of bad sectors. The following text can be found in the boot sectors in infected disks:

```
Welcome to the Dungeon (c) 1986 Brain & Amjads (pvt) Ltd
VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of
millions of viruses who are no longer with us today - Thanks
GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching
program follows after these messages....$#@%$@!!
```

There are a number of major and minor variations in the actual wording, but the substance of the message remains the same. There is also a completely different message giving three telephone numbers.

Brain replaces the boot sector of a floppy disk with its own code and moves the original boot sector further up the disk. While the virus is in memory the boot sector looks normal, as the virus redirects any attempt to look at it and displays the original boot sector instead. The virus has no ill effects other than slowing down the floppy disk drive and making 7Kb of memory unavailable to DOS.

Variants

Ashar:

 Copyright © Dr Solomon's Software

An early version of ***Brain***. There are six variants where the ***Brain*** message is different.

Brainy (Warrier)

Type
Memory resident file virus.

Affects
COM files on execution. COMMAND.COM is avoided.

File Growth
1,527 bytes.

Description
The virus contains the text **`The WARRIER!`**.

Brasil

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
The virus occupies two sectors. The first sector is an infection routine and the second is a resident interrupt handler and payload. The first sector is not stored in memory and is only read from the hard disk when the virus infects a floppy disk.

On the hard disk, the virus resides in the partition sector (cylinder 0, head 0, sector 1) and in the next sector (cylinder 0, head 0, sector 2). The original partition sector is stored in cylinder 0, head 0, sector 3.

No strings are visible in the virus. The encrypted string **`Brasil virus!`** is stored in the virus.

Copyright © Dr Solomon's Software

On floppy disks, the virus stores itself in the boot sector. The second part of the virus and the original boot sector of the floppy disk are stored in the last two sectors of the root directory (cylinder 0, head 1, sectors 14 and 15 for a 1.44Mb floppy disk).

The virus has a payload. It prints the message **`Brasil virus!`** and erases the sectors on track 0 of the hard disk. The trigger depends on many factors (for example, frequency of disk access, timer counter contents, and internal virus counter).

Burger

Type

Overwriting file virus.

Affects

A COM file on execution of an infected file. Some variants also infect EXE files.

File Growth

Most of the ***Burger*** variants are 560 bytes long, but this is unlikely to be noticed as the virus overwrites the start of the file.

Description

The virus overwrites the original program. The 792 version overwrites the first five sectors of drives C, A, D and B (in that order) if the system date is after February 1988. In one of the 560 versions, two random sectors of the first 256 are overwritten. In many other versions part of drive C is overwritten.

Most infected programs no longer run.

Variants

382, 405.a, 405.b, 542.a - d, 560a to 560.m, 1310.

Burger-405

Type

Overwriting file virus.

Affects

A COM file on execution of an infected file.

File Growth

Files of less than 405 bytes grow to that size. Files of greater than 405 bytes do not change but no longer function.

 Copyright © Dr Solomon's Software

Description

Infected programs no longer run.

Burglar.1150 (GranGrave.1150)

Type

Memory resident file virus.

Affects

EXE files.

File Growth

1,150 bytes

Description

The virus uses stealth to conceal itself when memory resident. It is a fast infector; not only infecting on execution, but sometimes also all EXE files in the current directory if just one program is run from that directory (if the minute of the current hour is less than 15).

If an EXE file has a valid NE header (is a 16-bit Microsoft Windows executable) the virus will not infect it. The virus avoids infecting files shorter than 256 bytes, or longer than 384Kb. In addition, the virus also avoids infecting some anti-virus programs.

The virus occupies 1,376 bytes of memory. It intercepts the following functions of interrupt 21h: 11, 12, 1a, 36, 3d, 43, 4b, 6C. The virus checks for itself in memory by issuing a call, AX=F078/INT_21h; the correct response is AX=0000.

For self-recognition of infected EXE files, the virus compares bytes at offsets 12h and 14h (the first belongs to the file checksum, the second to the start IP). If an XOR operation on these two bytes gives the value 78h, the file is considered to be already infected. Infected files also have 62 seconds in the time-stamp.

The virus contains the following strings:

```
AT THE GRAVE OF GRANDMA....
CLHWTBF-WCTK.
```

Copyright © Dr Solomon's Software

Butterflies (Goddam Butterflies)

Type
File virus.

Affects
COM files.

File Growth
302 bytes.

Description
This virus was originally spread via a couple of infected files that they were widely copied around, especially via BBS and the Internet.

This virus is not very infectious and is likely to die out unless it gets a similar boost once again.

Variants
There are three variants, the only difference being the text inside them (which is not displayed). The three texts are **`Goddam Butterflies, Hurray the Crusades,`** and an offensive message about a person.

Butthead

Type
File virus.

Affects
-

File Growth
-

Description
This virus seems to be a variant of *Cruncher.*

It contains the text:
`BUTTHEAD v 1.0 Automatic Compression Utility Written by The Cocanium Twilight Hell (c) 1994 Greetings to Eastwave BBS II, hoping he'll get killed!!!!`

Copyright © Dr Solomon's Software

ByeBye (Bye)

Type

Boot Sector Virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

ByeBye contains the following encrypted string **`Bye by C&CL.`**

The hard disk is infected by booting (or attempting to boot) off an infected floppy. Any subsequent floppy disk which is accessed will become infected by the virus.

Byway (Dir2.Byway, HndV)

Type

Memory resident file virus.

Affects

Files in a directory when the directory is accessed.

File Growth

-

Description

Unlike most file viruses, ***Byway*** does not add its code directly to infected files. It spreads by manipulating the way files are accessed under DOS. When an infected file is run, the virus goes memory resident and creates a file called CHKLIS T .MS (with spaces after the T and S, using the 'space' character [ALT-255] from the extended ASCII character set) in the root directory, with hidden, system and read-only attributes. It is this file which contains the virus code, and infected files are cross-linked to this file. The virus infects files in a directory when the directory is accessed (this includes directories accessed via the search path). The cross-linking is detectable if a clean copy of CHKDSK is run after a clean boot from a DOS system disk. If CHKDSK is run with the virus in memory, however, the virus uses stealth to conceal the cross-linking.

Copyright © Dr Solomon's Software

If the current DOS date is set to the year 1996 or in the future, and the day of the month is equal to the month's number times 2 and plus 2 (for example, 04-01-96, 06-02-96, ...26-12-96), the virus can trigger. When triggered, every 3 hours, on hours that are a multiple of three (for example, 09:00, 12:00, 15:00), the virus displays a running text string:

```
TRABAJEMOS TODOS POR VENEZUELA !!!
```

Literally translated, this means 'We are all working for Venezuela'. It is accompanied by a tune, possibly Venezuela's state anthem.

Cara

Type

Memory resident file virus.

Affects

COM files on execution, opening, renaming, or attribute change.

File Growth

1,025 bytes.

Description

The text **CARA** can be found near the start of the virus. The following strings can also be found:

```
Virus Es en memoria!
Disco Es infectado. Reemplaza Boot.
Clandestino Auto-Reproductivo Anti-virus
```

On every fourth access of a floppy disk, the virus checks the boot sector at offset 100h. If it finds one of six 2-byte signatures, it replaces the code of the boot sector with a non-infective one. *Brain, Italian* and *Stoned* are three viruses which this will clean. If it finds that memory is not a multiple of 16Kb, it displays **`Virus Es en memoria!`** followed by **`Clandestino Auto-Reproductivo Anti-virus`**.

Carioca

Type

Memory resident file virus.

Affects

COM files on execution (except COMMAND.COM).

 Copyright © Dr Solomon's Software

File Growth
951 bytes.

Description
If the system year is 1989 or later, the month November or December, and the date the 15th or later, the trojan is enabled. Every time a key is pressed the memory refresh timer is re-programmed so the refresh takes longer and longer. Eventually the refresh takes so long the system hangs.

Cascade (Second Austrian, 1701, 1704, Blackjack, Autumn, Waterfall, Russian, Hailstorm, Unk)

Type
Memory resident file virus.

Affects
COM files on execution, including COMMAND.COM.

File Growth
1,621 to 1,706 bytes, depending on variant.

Description
If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed. *Cascade* takes up 2Kb of memory when resident.

If the system date is between October and December 1988, or the virus goes memory resident when the year is 1980 and the year is subsequently set to 1989 or later, the virus produces a falling character display at random intervals. Characters detach themselves from their proper place on the screen and fall to the bottom of the display. As each character starts to fall the speaker clicks, so that the overall effect is rather like a hailstorm of characters.

This virus uses one of the interrupts which Novell Netware requires, and can cause serious problems on Novell Netware networks.

This is a very infectious virus. However, as the main variant has passed its trigger date it is difficult to detect without anti-virus software. The virus is encrypted to prevent casual disassembly and to fool automatic programs searching for virus characteristics.

Copyright © Dr Solomon's Software

Variants

17Y4, 1704-A, 1704-B, 1704-C, 1704-D, 1704-Format, 1621, 1661, and also a few minor variants of the **1701** version.

Casino

Type

Memory resident file virus.

Affects

COM files on execution. COMMAND.COM files of greater than 62,905 bytes and those with the system attribute set are avoided.

File Growth

The file size is rounded up to the next multiple of 16 bytes and 2,330 bytes are added.

Description

When an infected program is run it infects the first COM file in the sub-directory and creates a hidden file called COMMAND(ff).COM where (ff) is the invisible character 0FFh. This file is used by the virus to go memory resident, and then deleted.

The increase in file size is masked if the virus is in memory. This is not always precise as the virus subtracts 2,330 bytes from the file size if the file is a multiple of 16 bytes (unless the file size is less than 2,330 bytes), so some uninfected files appear smaller than they really are.

On the 15th of January, April and August the trojan triggers. The first 80 sectors of the current drive are read into memory; this includes the whole of the first copy of the FAT and normally part or all of the second copy. Garbage is written to the same 80 sectors. Then the following message is displayed:

```
DISK DESTROYER A SOUVENIR OF MALTA I have just DESTROYED the
FAT on your Disk!! However, I have a copy in RAM, and I'm
giving you a last chance to restore your precious data WARNING:
IF YOU RESET NOW, ALL YOUR DATA WILL BE LOST - FOREVER!! Your
DATA depends on a game of JACKPOT CASINO DE MALTE JACKPOT

CREDITS : 5

£££ = Your Dsk

??? = My Phone No.

ANY KEY TO PLAY
```


Copyright © Dr Solomon's Software

When you play, there are three possible results:

1. `HA HA !! You asshole, you've lost: say Bye to your Balls ....`

and the machine hangs.

2. `No Fuckin' Chance; and I'm punishing you for trying to trace me down !`

followed by the first message and a machine hang.

3. `BASTARD ! You're lucky this time - but for your own sake, now SWITCH OFF YOU COMPUTER AND DON'T TURN IT ON TILL TOMORROW !!!`

and the FAT is copied back on to the disk.

Casper

Type
File virus.

Affects
A COM file in the current sub-directory on execution of an infected file.

File Growth
1,200 bytes.

Description
If the virus tries to infect a write-protected disk the DOS `Write protect error writing drive X: Abort, Retry, Ignore?` message is displayed.

On April 1st the virus formats track zero of the floppy disk in Drive A. There is a message in the virus:

`Hi! I'm Casper The Virus, And On April The 1st I'm Gonna Fuck Up Your Hard Disk REAL BAD! In Fact It Might Just Be Impossible To Recover! How's That Grab Ya! <GRIN>.`

This message is part of the encrypted code, so it will not be visible in the virus. The virus was checked by setting the date to 1st April and running an infected program, and it did format track zero, head zero of the floppy drive; the hard disk was untouched. But because the registers were pointed to a non-legal track buffer, the disk was unreadable.

Variants
This virus is derived entirely from *Chameleon* but the second layer of encryption is not present.

Copyright © Dr Solomon's Software

Catman

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus includes the text string:

```
********************VIRUS PRODUCT

BY WATCHIRA EM KMITNB V3.0 HIGH SPEED SEE YOU AGAIN IN NEW
VIRSION

DATA 9:1989  *************************
```

Cawber.2138 (Baclab, NTU.T4, T4)

Type

Memory resident file virus.

Affects

EXE files (but files shorter than 2,000 bytes are not infected).

File Growth

2,138 bytes.

Description

Cawber uses steatlh to conceal itself when memory resident and is encrypted.

The virus intercepts INT_21h functions 11 (FCB findfirst), 12 (FCB findnext), 33, 3d (open), 3e, 3f, 40, 4202, 46, 4b00 (execute), 4e, 4f. When intercepting the DOS interrupt, the virus inserts a far jump on itself in the core DOS function dispatcher.

All infected files have starting IP=46h, SP=9FAh and the seconds field in the time-stamp is set to 30 seconds.

The virus contains two short strings:

`T4` (at the very beginning of virus body, unencrypted) and **`Griffe`** (encrypted).

 Copyright © Dr Solomon's Software

In addition, there is a long (encrypted) text message:

```
T4 virion ÄÄÄÄÄ  by NTU BACTERIOPHAGE LA
There Once Was A King, Who Called For The Spring
For His World Was Still Covered In Snow
But The Spring Had Not Been, For He Was Wicked And Mean ...
Here I'm Sitting And It's Getting Cold
The Morning Rains Against My Window Pane
While The World Looks So Cold And Grey
In My Mind I Dream Away
Then I'm On My Way To Tropic Islands
You'd Always Say I Was A Dreamer
You Were Right
What Do I Say When It's All Over ?
And SORRY Seems To Be The Hardest Word ...
```

When the payload triggers (this should happen after 13 January) the virus writes the above text at the beginning of some EXE files. They apparently hang when run.

Chameleon (1260)

Type

File virus.

Affects

A COM file in the current sub-directory on execution of an infected file.

File Growth

Approximately 1,260 bytes.

Description

This virus is based on a version of the *648* virus that was published in a book. It is written by the same author as *V2P6* – Mark Washburn of the USA. It appears to have been written to challenge anti-virus researchers, and has been encrypted on several levels so that it is very resistant to anti-virus techniques. It was the first polymorphic virus.

Copyright © Dr Solomon's Software

If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

Variants

V2P2 and *Casper* are very similar.

Chance.B (Lennon)

Type

Memory resident boot sector virus.

Affects

Floppy and hard disks.

The virus takes 1Kb of RAM. It infects floppy disks in drive A only.

File Growth

-

Description

The virus takes two sectors. On the hard disk, the virus is in the boot sector and in sector 3 on track 0. The original boot sector is saved in sector 2 of track 0. Boot sector-reads are stealthed.

On December 8th, the virus plays a Lennon/McCartney tune and prints:

`All we are saying is give peace a chance (J. Lennon)`

This message is encrypted in the virus body and is not visible.

On 1.4Mb floppy disks, the original floppy disk boot sector and the second sector of the virus are stored in the last two sectors of the root directory (cylinder 0, head 1, sectors 14 and 15). On 720Kb floppy disks, it is on cylinder 0, head 1, sectors 4 and 5.

Changsha (Centry)

Type

File virus.

Affects

COM and EXE files.

File Growth

-

 Copyright © Dr Solomon's Software

Description

The virus is not memory resident. It has no stealth capability and is very visible. The virus is not encrypted. The virus overwrites infected files.

Variants

3072 and **a**.

Chaos (Faust)

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

COM: 1,181 bytes.

EXE: 1,184 to 1,199 bytes.

Description

On the 13th of each month, the virus sets up two conditions:

It counts 50 keystrokes and then displays **`CHAOS!!! Another Masterpiece by Faust!!!`** and hangs the PC.

It sets up a trojan on the disk interrupt, so that every fifth disk access causes one track to be overwritten.

This is related to *Jerusalem*.

Variants

There are four minor variants, including **1241**.

Chill.554

Type

Memory resident file virus.

Affects

COM files.

File Growth

544 bytes.

Copyright © Dr Solomon's Software

Description

This infects COM files only, by appending itself to the end of the host file. The virus is encrypted. It is a fast infector, intercepting EXEC, open and rename/move DOS functions.

Chill.554 uses 1232 bytes of DOS memory (4dh paragraphs). It uses AX=7890h/INT_21h -> AX=7891h for self-recognition in memory. For self-recognition in files, the virus checks to see if the initial JMP points to exactly 554 bytes before the end of the file.

The virus has a payload, which is supposed to format the hard disk drive using AH=5/INT_13 function. This command is not recognised by IDE and SCSI drives (it can only affect some old MFM drives), so the virus doesn't do any damage.

It contains the following string inside:

```
[CHiLL TOUCH].You cannot touch these phantoms.
```

Chinese Fish (Fish Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus infects the partition sector of hard disk when the PC is booted from an infected floppy disk. Then it infects floppy disks on read or write access (for example, the DIR or COPY commands).

On hard disks, the virus stores its code on the partition sector, and re-locates the original partition sector to cylinder 0, head 0, sector 10. On floppy disks, it re-locates the original boot sector to track 79.

When active in memory, the virus stealths both the infected partition sector and the infected boot sectors of the floppy disk. It also stealths its own additional code.

If a disk infected with ***Chinese Fish*** is then infected with ***Stoned, Chinese Fish*** is able to remove some variants of ***Stoned,*** leaving it infected with just itself.

 Copyright © Dr Solomon's Software

Chinese Fish does not work under DOS 6 and will cause the machine to hang if run under this Operating System.

Starting in 1992, on the 1st, 11th, 21st and 31st of every month, when a PC is booted from an infected disk, the virus displays the following message:

```
Hello! I am FISH, please don't kill me. Congratulate 80th year
of the Republic of China Building,Fish will help to kill stone
Written by Fish in NTIT. TAIWAIN  80.10.18.
```

Choinka (Vienna-1881)

Type
File virus.

Affects
A COM file whenever an infected program is run. Only files between 10 and 60,000 bytes are infected.

File Growth
1,881 bytes.

Description
Between December 19th and 31st it displays its Christmas message – a large full-screen Christmas tree made of asterisks, and the message:

```
Merry Christmas & a Happy New Year for all my lovely friends
from FATHER CHRISTMAS.
```

When a key is pressed the host program is run. This is yet another version of *Vienna.*

Cinderella

Type
Memory resident file virus.

Affects
COM files on execution.

File Growth
390 bytes.

Description
The text `cInDeReL.1a` can be found in the virus.

Copyright © Dr Solomon's Software

After 30,000 calls to interrupt 16h (the keyboard handler), not counting function 0 (read a character), a hidden file with the name CINDEREL.1A is created, containing 0 bytes.

Clipper (Jeru-Clipper)

Type
Memory resident file virus.

Affects
COM and EXE files on execution.

File Growth
1,413 bytes. EXE files are first rounded up to a multiple of 16.

Description
The text **CLIPPER** can be found in the virus.

On the 16th of each month, if an infected program is run, the virus sets a flag when it goes memory resident. The next time a program is run it triggers the trojan, which overwrites the current drive, starting with the boot sector.

This is based on *Jerusalem*.

Coffeeshop

Type
Memory resident file virus.

Affects
EXE files.

File Growth
-

Description
There are two variants of this virus. **Coffeeshop.MtE** is a polymorphic virus using the MtE polymorphic generator (Mutating Engine).

Coffeeshop.1568 is almost the same virus, but this variant is not even encrypted (and apparently it has no built-in MtE generator). Both viruses infect EXE files when they are executed or copied; and neither variant works on DOS versions below 3.10.

Coffeeshop intercepts INT_21 functions 4B00 (Execute), 6C00 (Extended Open).

 Copyright © Dr Solomon's Software

To detect itself in memory, the virus issues a call, AX=33DA/INT_21; the correct response is AL=A5. It contains a filename recognition string (to avoid infecting anti-virus programs, the first two letters of the name are used; for example, SCAN, CLEAN, VSAFE, etc.):

```
SCCLVSNEHTTBVIRAFEMTBR
```

Coffeeshop contains a message, which is displayed on Friday if, when an infected program is run, the seconds counter is zero and the virus is not yet memory resident. The first string is encrypted, but the next two are visible, in memory:

```
LEGALIZE CANNABIS
Amsterdam = COFFEESHOP!
MK1992
```

Variants

Mte, 1568.

Com2Con

Type

File virus.

Affects

The next un-infected COM file in the current directory, when an infected program is run. Date and file attributes are preserved, but infected files have the time set to 11:19.

File Growth

311 bytes.

Description

There is a 1-in-4 chance of COMMAND.COM being renamed to COMMAND.CON if it is in the current directory when an infected program is run. If this happens to the COMMAND.COM needed at start-up, the '**`Bad or missing command interpreter`**' message is displayed when the PC is next booted.

CPW (Mediera, Mierda)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects
COM and EXE files.

File Growth
-

Description
CPW-1527 virus was first examined in February 1993, it was temporarily given the name 'Viva' but is now called **CPW**.

Infection takes place if a file is run or opened, or if any of its attributes are changed. It will not infect a file smaller than about 10K. It seeks out and infects COMMAND.COM by name when it first goes resident. If it cannot infect a file because a disk is write protected, it hangs the computer. When the system clock reads May 27, September 11, or December 28, it deletes the first file in the current directory every time a program is run.

Most of the virus is encrypted, including several messages. The messages are not displayed. When decrypted, the following text can be seen.

```
CPW fue hecho en Chile en 1992, -VIVA CHILE MIERDA!
```

Then the filespec used to seek out COMMAND.COM:

C:.COM

Next, some file names of common anti-virus software programs are listed. These are probably used to avoid infecting anti-virus programs.

```
GUARD guard CPAV SCAN CHKVIRUS CLEAN TOOLKIT VSAFE CHKLIST.CPS
```

Variants
1527

There is another variant called **CPW-1459**. It seems quite different from **CPW 1527**, lacking both encryption and the targeting of anti-virus software.

Crazy Boot

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

 Copyright © Dr Solomon's Software

File Growth

-

Description

The virus uses 3Kb; and uses stealth to conceal itself when memory resident.

The virus infects the partition sector and writes additional code to cylinder 0, head 0, sectors 4 and 5. On a floppy it infects the boot sector and writes additional code to cylinder 0, head 1, sectors 4 and 5.

The virus contains a message:

```
Don't PLAY with the PC!
Otherwise you will get in 'DEEP,DEEP' trouble!...
Crazy Boot Ver. 1.0
```

This message is displayed, depending on the state of an internal virus counter.

Crazy Daisy

Type

Trojan.

Affects

-

File Growth

-

Description

When the program is run, an animated face in block graphics appears at the top left of the screen. When a key is pressed, this message is displayed:

```
Hi, I'm Crazy Daisy! I'll format your HARDDISK! Say Goodbye to
Your files! Formatting...
```

The hard disk light flashes. The trojan is creating a large hidden file of between 200 and 400Kb with a randomly chosen name, and containing **`Keep smiling! - Sun is shining!`** over and over again. It then displays **`ERROR: No SYSTEM found! No files on drive C: Insert SYSTEM disk in drive A: and push any key!.`** If you do this, the virus patches every EXE file. When a patched program is run, it chooses one sentence at random, and each time a key is pressed displays another from its list. These sentences are:

```
Pretty day today - isn't it?
```

Copyright © Dr Solomon's Software

```
Don't worry - sing a song!

Life isn't easy!

Don't hate Your PC! Let's be friends!
```

Crazy Eddie

Type
Multipartite virus.

Affects
The partition sector when an infected file is run, and COM and EXE files on execution after the PC is started from an infected hard disk.

File Growth
2,600 to 2,700 bytes.

Description
The string **`Crazy Eddie`** can be found in the virus.

On June 28th, or any Monday 28th, the virus trashes the hard disk by writing garbage to it.

Variants
There is a corrupted version which does not work.

Crew 1 (V2480)

Type
File virus.

Affects
A COM file on execution of an infected file.

File Growth
2,480 bytes.

Description
The text strings below are in the virus.

After 1988, if the month is later than June, any infected program run results in a 3% chance that the following will be displayed:

```
This program is cracked by
```

 Copyright © Dr Solomon's Software

```
Notice this:
TS ain't smart at all.
Europcan
Crackin'
Crew
Distribution since
11-06-1987 (or 06-11-1987)
Press any key
```

Variants

Crew 2, with a length of 1,967 bytes.

Cruel

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This virus seems to have a Hungarian origin. Unlike most boot sector viruses, the virus infects the boot sector of hard disks rather than the partition sector. It also infects the boot sector of floppy disks.

DaBoys (Da'Boys, Dallas Cowboys)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Copyright © Dr Solomon's Software

Description

Unlike most boot sector viruses, the virus infects the boot sector of hard disks rather than the partition sector. The virus does not store a copy of the original, clean boot sector.

The virus also infects the boot sector of write-enabled floppy disks in drives A and B on any access, (for example, DIR or COPY commands).

Any software using interrupts 87-C6 is likely to hang the PC.

Damage (Diamond-Damage)

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

1,063 bytes. This is concealed if the virus is memory resident.

Description

The text **`DAMAGE!!!!`** can be found near the end of the file.

On Tuesdays, if an infected EXE file is run, the virus low-level formats the third floppy disk drive (probably meant to be the hard disk). The other effect is a large multi-colored diamond in the center of the screen, which shatters into smaller diamonds that bounce around the screen.

Variants

Damage-b:

The strings **`Jump for Joy!!!`** and **`DAMAGE-B!!`** can be found near the end. The damage routine covers floppy disk drives A and B and the third floppy drive. Files grow by 1,110 bytes.

Danish Tiny (Kennedy)

Type

File virus.

Affects

All COM files in the current sub-directory on execution of an infected file. If the virus

 Copyright © Dr Solomon's Software

tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

File Growth

333 bytes.

Description

When the date is June 6th, November 18th or November 24th, the message **`Kennedy Er död - laenge leve The Dead Kennedys`** is displayed, then the infected program is run. The dates are anniversaries of the deaths of members of the Kennedy family.

One of a long series of ***Tiny*** viruses, with lengths of 163 to 1,000 bytes.

Dark Avenger 1800 (Eddie-1, Black Avenger, Diana)

Type

Memory resident file virus.

Affects

COM and EXE files (see Description). Only works on MS-DOS v3.0 and higher. Only files of greater than 1,800 bytes are infected.

File Growth

1800 bytes, subject to a rounding-up to the nearest 16 bytes.

Description

A number of different actions on a file can trigger an infection:

1. If copied, both the source and target are infected.
2. If it is read.
3. If the attributes are changed.
4. If it is executed.

Read-only files are made read-write, and the attribute is reset after infection. The boot sector is used to store data.

The virus writes a sector that starts **`Eddie lives...somewhere in time!`** at intervals to a random sector on the hard disk. This sector might overwrite any sector on the disk including blank sectors, a sector of program code or part of a data file. The damage is therefore subtle, and may escape detection for some time. Any backup taken will include this corruption.

The virus includes two other messages which are not used:

Copyright © Dr Solomon's Software

`This program was written in the city of Sofia (C) 1988-89 Dark Avenger`

and

`Diana P.`

Variants

Dark Avenger 2 (Eddie 2):
Files increase by 651 bytes. There is no payload, but the string **`Eddie lives`** can be found in the code.

Dark Avenger 2000 (Eddie 3, V2000, Die Young, Traveller):
Files greater than 1,958 bytes are infected and grow by 2,000 bytes. When a program containing a copyright message from Vesselin Bontchev is run the system hangs (Vesselin Bontchev is a Bulgarian anti-virus researcher). It was first found in Bulgaria, contains the text **`666`**, as in the *512* virus, and uses many of the same ideas. In one version of the virus, the text **`Copy me - I want to travel`** is displayed. In another, it is **`Only the good die young...`**.

Dark Avenger 2100 (Eddie-4, V2100):
Files grow by 2,100 bytes (concealed if the virus is in memory) and the virus contains the text **`Eddie Lives`**. It uses interrupt 13h to corrupt the disk by writing garbage to random sectors. There are two versions: one uses the SI register at various places, the other uses the DI register. It is a development of **Dark Avenger 1** and **Dark Avenger 3.**

Ps!ko:
This is a simple hack of *Dark Avenger 1800*, the messages being replaced with **`The Ps!ko Virus - Version 1.0, SiTT and The Ps!ko Virus - Written in the USA, (C)1991 by SiTT and The Violator.`** A mistake in re-assembling the virus means that it can replicate only to one generation (2nd generation samples do not replicate).

MIR:
Infected files grow by 1,745 bytes. Near the start is the text **`#.I.R.*-*-*-* Sign of the time!`**.

1801:
A variant with a slightly different size.

1530, Milena, Slowdown:
In the **1800** version there are also slight variants **a, b, c, d, e, Rabid** and **Evil**.

 Copyright © Dr Solomon's Software

Dark Avenger Slowdown (V1028, Slowdown)

Type
Memory resident file virus.

Affects
COM and EXE files on execution. Only files of greater than 1,028 bytes are infected.

File Growth
COM: 1,028 bytes.

EXE: 1,028 to 1,043 bytes.

Description
The PC is slowed down, and the slowing is proportional to the time of day. At midnight there is no slowing, at 1 a.m. there is one loop of repeatedly executed instructions, at 2 a.m. there are two loops, and so on.

Dark Lord

Type
Memory resident file virus.

Affects
COM and EXE files on execution or closing. COMMAND.COM is avoided. The date and time are not preserved.

File Growth
Rounds up to a multiple of 16 bytes, then adds 921 bytes.

Description
The strings **`Dark Lord, I summon thee!`** and **`MANOWAR`** can be found in the virus.

Interrupt ECh is defined as the old interrupt 21h.

Darth

Type
Memory resident file virus.

Affects
COM files on execution. COMMAND.COM is avoided.

Copyright © Dr Solomon's Software

File Growth
None.

Description
The virus goes memory resident by finding an area of zeros in the segment from 9000h, copying itself there and patching the DOS function despatcher to change the effect of function 40h (write to file). Thereafter, when a file is written to, the virus overwrites the first 253 bytes of that file. Then the files no longer work.

The string **`Darth Vader`** can be found in each version of the virus.

Variants
Darth Vader-2:
This checks for 345 zeros in the file. If it finds that many, it writes itself into the file.

Darth Vader-3:
This needs only 255 bytes of zeros.

Darth Vader-4:
This needs 200 bytes of zeros.

Datacrime (Columbus Day)

Type
File virus.

Affects
A COM file on execution of an infected file. Files with D as the seventh letter (including COMMAND.COM) are not infected.

File Growth
1,168 bytes.

Description
When an infected file is run, the virus scans through the directory tree for an uninfected file. It also searches DOS devices in the order C, D, A, B. It recognizes infected files by setting the last byte of the seconds field in the directory entry, which is not displayed by the DIR command.

Every year from October 13th to December 31st, when it runs it displays the message **`DATACRIME VIRUS RELEASE 1 MARCH 1989`** and does a low-level format of the hard disk of cylinder 0, heads 0 to 8. If it tries to infect a write-protected disk, the DOS write-protect message is suppressed. The virus handles this incorrectly, and the next critical error encountered by DOS can crash the machine.

 Copyright © Dr Solomon's Software

Variants

Datacrime 1b:
Files grow by 1,280 bytes.

Datacrime 2, 2b:
Both COM and EXE files are infected. COM files grow by 1,480 bytes and EXE files by between 1,500 and 2,000 bytes. When the virus triggers, it displays **`DATACRIME II VIRUS`**.

Datalock

Type
Memory resident file virus.

Affects
COM and EXE files on opening or execution.

File Growth
920 to 1,043 bytes.

Description
Contains the text **`DataLock version 1.00`**.

When any file called *.?BF is opened on any date after August 1990 the machine hangs (although it was intended to do something else).

Variants
a, b, c, d, e , f. The **f** version is 1,043 bytes long; all the others are 920 bytes long.

David (Diamond-David)

Type
Memory resident file virus.

Affects
COM and EXE files on execution. COM files of greater than 63,851 bytes are not infected.

File Growth
1,173 bytes. The increase is hidden using stealth.

Copyright © Dr Solomon's Software

Description

Because of a bug, infected COM programs do not work and are corrupted instead of being infected.

The text **`(C) David Grant Virus Research 1991 PCVRF and Distribuite this virus freely!!! ... ah ... John ... Fuck You!`** can be found near the start of the virus.

Because of the stealthing of file size, when CHKDSK is run with the virus active in memory, it will report inconsistencies between the sizes of infected files and the length of the FAT chain. If the PC is booted from a clean DOS disk and CHKDSK is run, the virus cannot stealth the file size and no inconsistencies are reported.

On Tuesdays, the virus tries to format the hard disk but fails because of a bug.

Dbase (DBF)

Type

Memory resident file virus.

Affects

COM files on execution. Date/time and attributes are preserved.

File Growth

1,864 bytes. 1,884 bytes are subtracted from the top of conventional memory. This can be shown using CHKDSK.

Description

If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

DBF files are garbled by interchanging pairs of bytes. The virus also creates a hidden file in the root directory called C:\BUGS.DAT which contains the list of garbled files. Three months after the file is created, a damage routine should trigger. The same thing happens if the system date is set to three months before the date of BUGS.DAT. The damage routine does not work because of a bug in the code. If it did, it would write garbage over the first 256 sectors on the hard disk, overwriting the boot sector, both copies of the FAT, and the whole directory. It would do this to every device attached to the PC, starting at drive D and working up to drive Z. On a system with no drive D the system would hang. On networks, the network software will not permit a direct write to the drive by DOS programs (including a virus).

 Copyright © Dr Solomon's Software

Deicide

Type
Overwriting file virus.

Affects
COM files in the root directory of drive C (except COMMAND.COM) on execution of an infected program.

File Growth
None. The first 666 bytes of the file are overwritten.

Description
The text **`DEICIDE! Glenn(666) says : BYE BYE HARDDISK!! Next time be carufull with illegal stuff.....`**. can be found near the beginning of the virus.

After each infection, the message **`File coruption error`** is displayed. If the virus cannot find an uninfected file to infect in the root of drive C, it overwrites the first 80 sectors of the drive.

Variants
Deicide-2 is a non-overwriting virus, infecting COM files and adding 1,335 bytes to them.

DelWin (Goblin)

Type
Multipartite virus.

Affects
EXE files (longer than 3,000 bytes) and the partition sector of hard disks.

File Growth
See variants.

Description
The virus occupies six sectors on an infected hard disk (on cylinder 0, immediately following the partition sector).

This virus uses 2Kb of RAM. It uses stealth to conceal itself when memory resident. It is also a fast infector, infecting files on open as well as on execution.

This virus has a payload; it shakes the screen when several months have passed since the installation of the virus on the partition sector.

Copyright © Dr Solomon's Software

Variants
1759, 1199.

Demon

Type
Overwriting file virus.

Affects
All COM files in the current sub-directory on execution of an infected file.

File Growth
None. The first 271 bytes of the file are overwritten.

Description
Because of the overwrite, infected programs no longer work normally. A text string in the virus says **`Demonhyak Viri X.X (c) by Cracker Jack 1991 (IVRL).`**

On Tuesdays, the virus overwrites the first 160 sectors of drives A to J and then displays **`Error eating drive C:.`**

Den Zuko 2 (Venezualan, Search, DenZuk)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
Once the virus is in memory, its infection counter (initialized to 8) is decremented every time a disk is accessed. When the counter reaches 0 the infection process is triggered and the counter is reset to 2.

On systems with a color monitor, when Ctrl Alt Del is pressed the text **`Den Zuk`** is displayed in red with a symbol to the side of the screen which looks like a stylized globe. The volume label of an infected disk is changed to Y.C.I.E.R.P.

 Copyright © Dr Solomon's Software

There are two text messages in the virus which are not displayed. At the beginning is **`Welcome to the Club -The HackerS- Hackin' All The Time`** and at the end is **`The HackerS`**.

Den Zuko replaces the boot sector of a floppy disk with a 360Kb boot sector of its own. This gives problems with floppy disks of a higher capacity. The virus also uses track 40, head 0, sectors 33 to 41 to store code and the bitmap of the logo. This has no ill-effects on 360Kb floppy disks, but will overwrite data on track 40 of any higher-capacity disk.

If the virus finds *Brain* or *Den Zuko 1* on the boot sector, it overwrites them with itself. If Ctrl Alt Del is pressed, a re-boot is triggered and the logo is displayed. *Den Zuko* marks the disk as *Brain*-infected, so that *Brain* will not infect it.

Variants

Den Zuko 1 (Ohio):
An early version. When a warm boot is performed a box is displayed containing the message **`(c) 1988, The HACKERS Technology Bandung 40254 - Indonesia.`**

Den Zuko 2.a:
-

Den Zuko 3:
When an infected PC is re-booted, a blue box is displayed in the center of the screen containing the message **`(c) 1988, The HACKERS Technology Bandung 40254 - Indonesia.`**

Desperado.1403

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

1,403 bytes.

Copyright © Dr Solomon's Software

Description

This is a fast infector, infecting files when they are executed or opened.

The virus does not infect files where the file size, divided by 16, gives a remainder of 3 (that is, if Filesize mod 16 = 3). This is a tricky way to recognise files which have already been infected. The virus also avoids infecting COM files shorter than 4096 bytes and longer than 60000 bytes.

Desperado uses 6KB of memory. It intercepts the following functions of interrupt 21h: 4B00, 3d, 6C. The virus is able to go resident in the UMB area of memory.

The virus checks for itself in memory by issuing a call, AX=4BFF/INT_21h; the correct response is BX=162E.

The virus deletes CHKLIST.MS files produced by Microsoft Anti-Virus (MSAV).

The following strings are contained within the virus:

```
Dr W-2
```

```
Dr White - Sweden 1993
```

```
Desperado Virus - Written in Malmo... F02E
```

(in place of F02E, variant **b** has F02D and variant **c** has F02C):

```
SCANCLEAVSHITOOLMSAVCPAVVSAFF-PRVIRSTBAV
```

```
TBSCTBCLTBUT-V  UTSCUT CHKLIST.MS
```

The last string represents the first four letters of the names of various anti-virus programs; the virus avoids infecting these programs.

Variants

a-c.

Destructor

Type

Memory resident file virus.

Affects

COM and EXE files on execution, opening, renaming, change of attribute or date/time access. COM files between 50 and 64,000 bytes are infected.

Copyright © Dr Solomon's Software

File Growth

COM: 1,150 bytes.
EXE: padded to nearest multiple of 16, then another 1,150 bytes are added.

Description

There are two text strings in the virus: **`DESTRUCTOR V4.00 (c) by ATA`** and **`The Time is my !.`** There is no payload.

Devil's Dance (941, Mexican)

Type

Memory resident file virus.

Affects

COM files on execution. The original date and time are not preserved.

File Growth

941 bytes each time they are infected. When they are greater than the 64Kb limit they will not run.

Description

Every time the infected PC is re-booted the following message is displayed:

```
Have you ever danced with the devil under the weak light of the
moon?
Pray for your disk!
The__Joker ...
Ha Ha Ha Ha Ha Ha Ha Ha Ha Ha
```

If you re-boot after the virus has gone memory resident and a few thousand keystrokes have been entered, the virus overwrites the partition sector with garbage after displaying the message. Next time the PC is started it will appear not to have a hard disk and after a few keystrokes each character will be displayed in a different color.

Variants

Devil's Dance.b:
The partition sector is not overwritten.

Copyright © Dr Solomon's Software

Dewdz

Type
File virus.

Affects
A COM file on execution of an infected file.

File Growth
601 bytes.

Description
The text **`Kewl Dewdz!`** and **`Made in STL (c) '91`** can be found encrypted in the virus.

Each time an infected program is run, there is a 21% chance that the virus will move the cursor to row 12 column 35, display **`Kewl Dewdz!`** and restore the cursor position.

Diablo (Diablo_boot)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk. The virus does not infect floppy disks of less than 1.2Mb.

The virus takes 2Kb of RAM. It infects floppy disks in drive A only.

File Growth
-

Description
The virus occupies one sector. The string **`DIABLO`** serves as a virus marker. It should be present at offset 1AAh.

The infected partition sector/boot sector always starts with EB 3C 90.

The original partition sector is re-located to cylinder 0, head 0, sector 2. The virus does not use stealth to conceal itself.

The original floppy disk boot sector is stored on cylinder 0, head 1, sector 14 (the root directory for a 1.44Mb floppy disk).

 Copyright © Dr Solomon's Software

The virus has no payload. It tries to avoid heuristic analysis by reducing the memory variable in the word at [0:413], by means of complex operations with the word at [0:412] and the byte at [0:414].

Diamond (V1024)

Type
Memory resident file virus.

Affects
COM and EXE files on execution. Date/time and read/write attributes are not changed.

File Growth
1,024 bytes. If the virus is in memory the growth is hidden from DIR commands.

Description
If the PC has a color monitor being used in text mode, the virus display triggers on the hour. This starts as a multi-colored diamond made up of four smaller diamonds in the center of the screen. After a brief pause the smaller diamonds scatter and bounce around the screen independently. Every time they pass over a character they blank it so the screen is gradually cleared except for the bouncing diamonds.

Variants
Diamond-b:
As above.

Die-Hard (DH2)

Type
Memory resident file virus.

Affects
COM and EXE files (**Die-Hard.3000** infects COM files only).

File Growth
See Variants.

Description
Die-Hard.4000 is a fast infector; and intercepts DOS functions: 3D (open), 6C (open/create), 4B00-4B03 (execute, load/execute), 3E (read), 4202 (lseek end). The virus uses stealth to conceal itself when memory resident. However, the DIR command

Copyright © Dr Solomon's Software

reports the file size correctly, because functions 11h/12h are not intercepted by a virus stealth routine. This variant occupies 9,232 bytes of DOS memory; on a PC having 640Kb of conventional memory, it is located in segment 9DC0h.

Die-Hard.4000 checks EXE files for the MZ signature only. This means it will corrupt any EXE file having a ZM signature, as it will be treated as a COM file.

Die-Hard.4000 contains the string:

```
SW DIE HARD 2
```

Die-Hard.4000 overwrites ASM files with a short assembler text. When compiled, the corresponding code hangs the machine.

Variants

3000, 4000a-c.

Die-Lamer.1098 (VLamix)

Type

Memory resident file virus.

Affects

EXE files.

File Growth

1,098

Description

Die-Lamer is a fast infector, infecting files being executed or closed. All infected files have the starting IP=10h. The virus is encrypted.

The virus uses INT_91h as an internal alias for INT_21h. It also intercepts INT_10h (video output), which is used for the payload.

The virus does not infect all files properly. Such files do not decrypt; as a result, FindVirus detects the files as 'is like *Die-Lamer.1098*' (the files are not repairable).

The virus contains the following strings:

```
smart*.cps chklist.* -=*@DIE_LAMER@*=- CHKLIST ???

CHKLIST.CPS

VLamiX-1
```

 Copyright © Dr Solomon's Software

The virus deletes CHKLIST.MS and CHKLIST.CPS files (and also SMARTC*.CPS files) produced by Microsoft Anti-Virus (MSAV) and Central Point Anti-Virus (CPAV).

This virus has a payload, which activates if the string

```
=*@DIE_LAMER@*=-
```

is being printed via INT_10h. If this is the case, the virus fetches a low-level disk access address using AH=13/Int_2Fh and erases a series of sectors on the floppy disk in drive B (if there is one).

DIR II (Creeping Death)

Type

Memory resident file virus.

Affects

COM and EXE files whenever their directory entry is accessed. As a result, this virus spreads very quickly.

File Growth

None apparent, but an extra cluster is loaded when the file is executed.

Description

When an infected application is run, the virus goes memory resident and copies its code to the last cluster on the partition. This is then marked as bad in the File Allocation Table (FAT). Subsequently, the virus infects by patching the directory entries of uninfected files. With the virus in memory, any file or directory activity will result in an infection; for example, use of the DIR on a directory will infect all the files in that directory.

The patching of the directory entries is done as follows. The original start cluster of the file is copied (and, at the same time, encryted) to bytes immediately preceding the date and time in the reserved area of the directory entry (between the file attribute and date and time). The start cluster in the directory entry is then patched to the cluster where the *DIR II* code is contained. When an infected program is run, DOS executes *DIR II* first, which then decrypts the original start cluster of the file and passes that to DOS to allow the program to execute normally.

DIR II uses advanced stealth to conceal itself when memory resident.

If the PC is booted from a clean DOS system disk and CHKDSK is run, a large number of files are cross-linked via one cluster (the cluster containing the DIR II

Copyright © Dr Solomon's Software

code). If the PC is booted from the hard disk, ***DIR II*** uses stealth to conceal the cross-linking; and CHKDSK reports no errors.

There are no effects, other than the cross-linking of infected files.

DIR II is not compatible with MS-DOS 6.x, one of the reasons for its decline in recent years.

Variants

There are a few minor variants, including **DIR II.a**.

Dirvir (Dir)

Type

Memory resident file virus.

Affects

An uninfected COM file when a DIR is requested.

File Growth

691 to 760 bytes. Growth is concealed if the virus is in memory.

Description

When an infected file is run there is a 1-in-256 chance that the first two sectors of the FAT will be overwritten with garbage.

Discom (Jeru-Discom)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. Files with names starting with ACAD are not infected.

File Growth

COM: 2,053 bytes.
EXE: padded to the nearest 16 bytes, then another 2,053 bytes are added.

Description

There is a counter in the last byte of the file. When this reaches 80 the trojan is

 Copyright © Dr Solomon's Software

triggered, which writes one sector of rubbish to the hard disk each time an infection takes place.

This virus is based on *Jerusalem*.

Disk Filler (Filler-6, Filler)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

When the PC is booted from an infected floppy disk, the virus infects the partition sector of the hard disk. When the PC is booted from the hard disk, the virus goes memory resident and infects each floppy disk accessed in any drive. On hard disks, the virus occupies cylinder 0, head 0, sectors 0 to 7, and on floppy disks, to the track after the last track.

The following text is in the virus:

Haha, varus van a gepben!! Ez egy eddig meg nem kozismert varus. De hamarosan az lesz. A neve egyszeren toltogeto. Ezt a nevet onnan kapta, hogy feltoltogeti a FAT-tablat kolonbozo alakzatokkal. Ez nar meg is tortent!!!

The virus uses stealth to hide the infected boot sector.

If 26 minutes pass without disk access, the trojan triggers. It overwrites the FAT with a picture that looks like this:

oooooo oooooo
o oo o
o o o oo o o o
o oo o
o oooo oo oooo o
o o o o
oooo oooo

Copyright © Dr Solomon's Software

The character used is ASCII 1 (the smiling face). Then the message is displayed.

Variants
Filler.a, Filler.b.

Doom II.1240 (Taiwan Doom II.1240)

Type
Memory resident file virus.

Affects
COM and EXE files on execution.

File Growth
1,240 to 1,255 bytes.

Description
The virus contains the encrypted text **`DOOM II (c) Dr.Jones, NCU.`**

Four sectors of drive C are overwritten. In March, there is a 1-in-6 chance that the first track of the hard disk will be overwritten each time an infected application is run. At the same time, the first track of each floppy disk currently in a drive is overwritten.

Doom II.752 (Taiwan Doom II.725)

Type
Memory resident file virus.

Affects
A COM file on execution of infected files.

File Growth
752 bytes.

Description
On the 8th of each month, the current hard disk is trashed, as are the first 320 sectors of drive D. It then displays **`DOOM I, (c) NCU Taiwan`**.

 Copyright © Dr Solomon's Software

Doteater

Type
Memory resident file virus.

Affects
A COM file of less than 63,488 bytes when an infected program is run.

File Growth
944 bytes.

Description
When COMMAND.COM is infected when the PC is booted, a face enters from the right-hand side of the screen and eats every dot you type, complete with sound effects. Pressing ^ cancels the effect.

DSME.Teacher (DSME.Demo)

Type
Memory resident file virus.

Affects
COM and EXE files on execution. COM files of greater than 50,152 bytes are not infected.

File Growth
Variable: 3,240 to 3,590 bytes.

Description
The virus is variably encrypted and highly polymorphic. There is no payload.

The virus contains the encrypted strings:

```
Teacher virus ( A demo virus for DSME to all teacher )
```
and
```
DSME v1.0.
```

Dyslexia (Solano)

Type
Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

A COM file on execution. Date/time and read/write/hidden attributes are preserved. COMMAND.COM is avoided.

File Growth

2,000 bytes.

Description

12.25 minutes after the virus goes memory resident it picks a random position on the screen. If there is a figure there and, in the position to the right, it swaps them. It repeats this every 73 seconds. This works on color and mono screens in text mode.

Variants

Dyslexia dropper:

This drops *Dyslexia* into memory. The dropper is not itself a virus, but once it is in memory every COM file run will be infected.

EDV

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

When the PC is booted from an infected floppy disk, the virus goes memory resident. While it is, any write-enabled floppy disk that is accessed is liable to be infected.

Hard disks become non-bootable, but accessible. Memory is not reduced, so memory map programs and monitors may not see this virus becoming resident. The message **`MSDOS Vers. E.D.V.`** can be found on infected boot and partition sectors.

The virus replaces the boot sector of a floppy disk with its own code and moves the original boot sector further up the disk. In the case of a hard disk, it moves the partition sector and replaces the original with its own code. While the virus is in memory, it counts the number of disks it infects, and after the sixth disk is infected the damage routine is triggered. The count is reset if the PC is re-booted before the sixth infection.

 Copyright © Dr Solomon's Software

The damage routine writes garbage over the first and second hard disk, then over the first four floppy disk drives. This means all drives on most PCs. The garbage is written to cylinders 0 and 1, heads 0 to 3. This will overwrite the partition sector, the boot sector, both copies of the FAT, and the directory, on most disks.

Then it displays **`That rings a bell, no? From Cursy`**. If the virus is in memory, it tries to hide itself. If you try to read the boot sector the virus displays the original sector, not its own code.

Eight Tunes (1971)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. COM files between 8,177 and 63,310 bytes and EXE files of greater than 8,177 bytes are infected. Date/time and read/write attributes are preserved.

File Growth

1,971 bytes.

Description

When a file is first infected, the virus stores the current date as the number of days since January 1st 1984. When an infected file is run and the system date is 91 days or more after that, it chooses a tune from a repertoire of eight and plays it about 30 minutes afterwards. The tune most likely to be recognized is 'Auld Lang Syne'. The others are 'Nobody Knows the Trouble I've Seen', four German rambling songs, a series of random notes, and the interrupt 8 handler re-interpreted as music. After it has played the first tune, it waits for a few minutes and repeats the choice of a random tune, then continues to play the tune every few minutes.

The virus does its own memory management, so may not be detected by monitors or memory map programs.

Empire (Evil Empire)

Type

Boot sector virus.

Copyright © Dr Solomon's Software

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
When the PC is booted from an infected floppy disk (not necessarily a bootable one), the virus copies itself to the hard disk. While the virus is present it infects any disks or disks that are accessed. There are a large number of variants, as the author of the virus kept changing it to evade the anti-virus detection system used by the University of Alberta.

Variants
1, 2, Botany, a, b, c, d, #2, Canadian, Non-Canadian, U of A, UA, B.4, B1, Evil, D1, D2.

Empire.Monkey (Monkey, Stoned. Empire. Monkey)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
The virus infects the partition sector of the hard disk when booted from an infected floppy disk. The virus then infects floppy disks accessed where the virus is memory resident.

This virus has no payload, and contains the encrypted string **`Monkey.`**

The virus encrypts the original boot sector (floppy disks) or the partition sector (hard disks) and does NOT store a copy of the original boot or partition sector anywhere on the disk (on hard disks, an encrypted copy of the partition sector is stored on cylinder 0, head 0, sector 3). When the PC is booted from the hard disk, the virus goes memory resident and decrypts the partition sector, so that the PC boots normally. If an infected PC is booted clean, the partition table remains encrypted and DOS is unable

 Copyright © Dr Solomon's Software

to access the hard disk (an attempt to access the hard disk by typing **C:** produces the message, **Invalid drive specification**).

For this reason, FDISK/MBR should not be used to remove this virus; if FDISK/MBR is used the hard disk will become inaccessible (the PC will fail to boot from the hard disk).

Variants

Empire.Monkey.B contains some pieces of code rearranged, but is otherwise almost identical.

Enigma

Type

File virus.

Affects

EXE files on execution of an infected file.

File Growth

1,755 bytes.

Description

Near the end of the virus is the text **This is the voice of the Enigma virus.....the spirits of the hell are coming back! (C) 1991 by Cracker Jack * Italy *.**

On Sunday or Monday it formats track 20, head 0 of the floppy disk in drive A and attempts to re-boot the PC. Some machines just hang.

This virus is a plagiarized version of *Old Yankee*.

Variants

Enigma.b:
The effects are triggered on Saturdays.

Espejo (15 Years, Stakka, Esto te pasa)

Type

Boot sector virus.

Copyright © Dr Solomon's Software

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
When the virus is memory resident, it infects any floppy disks accessed (for example, with the DIR or COPY commands).

On the 7th April, or any other date if the virus infected ten disks since the last boot, the virus triggers and switches to its destructive mode. Any disk being accessed after this is overwritten with the following text (in Spanish):

```
Esto te pasa por programas que a nosotros nos cuesta tanto
trabajo hacer. Que te quede de Experiencia, Mexico,1994
```

The virus also intercepts interrupt 16h (BIOS Keyboard Services). Then it occasionally simulates typographic errors by adding 5 to the character code being entered from the keyboard. For example, A changes to F, B to G, and so on.

The virus contains another text string:

```
This Virus is from MEXICO, I have 15 years old.
```

Etc

Type
File virus.

Affects
A COM file on execution of an infected file.

File Growth
700 bytes.

Description
The text **`Virus, (c) ETC`** and **`E.T.C.VIRUS, Version 3.0, Copyright (c) 1989 by E.T.C. Co.`** can be found in the virus.

The first time that the infected program is run, the message **`Virus, (c) ETC`** is displayed before the program runs.

 Copyright © Dr Solomon's Software

Evil (Live after Death 3, Phoenix Evil)

Type
Memory resident file virus.

Affects
COM files on opening, except those greater than 64Kb and some others (approximately one file in eight is ignored). Some EXE files are also trojanized.

File Growth
1,701 bytes. COMMAND.COM is infected without increase.

Description
The text **`The evil that men do lives on and on...`** is encrypted in the virus. The encryption and the decryptor/loader are both variable, so there is no consistent search string.

The FAT is gradually corrupted by the occasional swapping of two entries while they are in the sector buffer. This means anything monitoring disk-writes fails to see the corruption, as it happens in memory as DOS does the write. In addition, at interrupt 13h level some disk-reads are converted to writes.

Variants
This is part of a long series from Bulgaria.

Exebug (EXE_Bug, CMOS Killer)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk. In addition, under certain circumstances, an EXE file being written to disk (for example, on the COPY command) may be trojanized (see Description).

File Growth
-

Description
This stealth virus attempts to undermine a normal clean boot. When a PC is booted from an infected floppy disk, the virus infects the partition sector of the hard disk and patches CMOS to disable the A drive. Thus, when the PC is booted (including a boot from DOS system disk), the infected partition sector is loaded, the virus goes

Copyright © Dr Solomon's Software

memory resident and continues with a normal boot from the A drive. Then the virus infects any floppy disk which is accessed (for example, on the DIR command). Before attempting a clean boot, it is necessary to ensure that drive A is enabled in CMOS.

When memory resident, the virus infects floppy disks accessed (for example, with the DIR or copy commands), demonstrating stealth techniques, and concealing the changes made to boot and partition sectors.

When an EXE file is being written to disk (for example, LINK or COPY commands), under certain circumstances, the virus can trojanize the file.

EXE files being written to A can be trojanized to become the ***Exebug*** virus dropper. On execution, such a program deletes all the files in the current sub-directory, infects the hard disk, then terminates.

EXE files written to drives other than A can be turned into instant trojans, trashing all data on the hard disk when executed.

The virus patches CMOS to disable drive A to bypass the clean boot. Even if you set up CMOS to re-enable drive A and boot from a clean system floppy disk, the hard disk will be inaccessible at a DOS level since the virus overwrites the partition table in the infected partition sector. For this reason, FDISK/MBR should not be used to remove this virus; if FDISK/MBR is used the hard disk will become inaccessible (the PC will fail to boot from the hard disk).

Variants

There are a number of ***Exebug*** variants, including variants **a, b, c, d, e** and **EXE_Bug.Hooker**. Some of them do not disable drive A and thus cannot survive a clean boot.

Exterminator

Type

Overwriting file virus.

Affects

All COM files in the current sub-directory on execution of an infected file.

File Growth

None. Overwrites the first 451 bytes.

Description

Infected programs no longer work as they should. There is text in the virus which says:

 Copyright © Dr Solomon's Software

Exterminator 1.0 - (c) by Cracker Jack 1991 (IVRL) Italian Virus Research Laboratory (C) 1990,1991 Message to Virus Researchers: Non rompetemi le palle o mi arrabbio... Non so Se sono stato abbastanza charo... Exterminator Virus 1.0 (c) by Cracker Jack 1991 (IVRL) No panic...this is a Harmless Virus...

On Mondays, the virus overwrites the first 160 sectors of drive C. Then it displays **Exterminator Virus 1.0 (c) by Cracker Jack 1991 (IVRL) No panic...this is a Harmless Virus...**

F-You

Type
Memory resident file virus.

Affects
COM and EXE files on execution.

File Growth
417 to 635 bytes.

Description
The text, **'Fuck you!'** can be found in the virus.

Fifty-five minutes after the virus goes memory resident the screen clears and the message appears in the middle. It stays there for a while, then disappears and you can continue. This is repeated every hour.

F1-337

Type
Memory resident file virus.

Affects
COM files on execution or opening. COMMAND.COM is avoided.

File Growth
337 bytes.

Description
There is no payload.

Copyright © Dr Solomon's Software

Faggot

Type
File virus.

Affects
COM files on execution of an infected file.

File Growth
1,009 bytes.

Description
The virus contains the string **`Hi Guy! Nice to meet you! I an the little FAGGOT virus!`** and some obscene messages.

On 7th March, it is meant to format drive C, but this does not work. However, the virus trashes the hard disk (overwriting it with 800 sectors of garbage) before trying to infect a file: as a result, it never actually infects a file.

Falling Letters Boot

Type
Memory resident boot sector virus.

Affects
Floppy and hard disks, when booted from an infected floppy disk (not necessarily a bootable one).

File Growth
-

Description
The boot sector is moved further up the disk and replaced with the virus's own code. On floppy disks the boot sector is moved to cylinder 39, head 1, sector 6.

The virus triggers a falling letters display.

Fat Avenger

Type
Boot sector virus.

Copyright © Dr Solomon's Software

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The Virus is slightly unusual in that it occupies three sectors (usually boot sector viruses use 1 or 2 sectors). The virus contains the following string.

```
THIS PROGRAM WAS WRITTEN IN INDIA. (c) 1993 FAT AVENGER

PS. this program is not meant to be destructive
```

The virus appears to have been written in a high-level language - parameters for subroutines are passed through the stack, which is not common in virus writing.

Feint (INT 7F)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk. The virus does not infect floppy disks of less than 1.2Mb.

The virus takes 2Kb of RAM (the virus code is always in the segment 9F80). The virus will not work on PCs with less than 640Kb RAM.

File Growth

-

Description

The virus takes one sector. It uses interrupt 7F as a replacement of the original interrupt 13.

The original partition sector is re-located to cylinder 0, head 0, sector 2. The virus does not use stealth to conceal its own code.

The virus uses byte 42h in the boot sector as an infection marker. If it is 13h then the disk is considered to be infected already. The original floppy disk boot sector is stored in sector 3, head 2, cylinder 1.

The virus contains no strings and it has no payload.

Copyright © Dr Solomon's Software

Fichv.2_1 (905, CHV 2.1)

Type
File virus.

Affects
All COM files in the current sub-directory of greater than 1,500 bytes, when an infected file is executed.

File Growth:
896 to 903 bytes.

Description
The text **`FICHV 2.1 vous a Eu`** can be found in the virus.

During March it will trash the disk by writing the above message to the first six sectors of each track. The virus is encrypted and attempts to resist disassembly by using interrupts 1 and 3.

Variants
Version **1.0** infects EXE files, adding 897 bytes.
Version **2.0** infects COM files, adding 896 bytes.

Filedate 11 (USSR)

Type
File virus.

Affects
An EXE file on execution of an infected file. All infected files are given the date and time August 17 1988, 2:08 a.m.

File Growth
571 to 586 bytes.

Description
Every time an infected program is run there is a 3% chance that it will overwrite the partition sector of the hard disk.

Filehider 11 (V789)

Type
Memory resident file virus.

 Copyright © Dr Solomon's Software

Affects
COM files on execution. Only files of less than 63,488 bytes are infected.

File Growth
789 bytes.

Description
Every Friday there is a 1-in-16 chance of the trojan triggering. On Friday 13th this becomes a 1-in-4 chance. The trojan makes all files in the current sub-directory hidden.

Findme

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
Findme occupies just one sector. It uses 1Kb of RAM and goes resident at the top of memory (below 640Kb).

The original partition sector is re-located to cylinder 0, head 0, sector 16. The virus uses stealth to conceal both the infected partition sector, and the re-located original sector (0, 0, 16 looks blank when examined with the virus memory resident). The infected partition sector does not contain a valid partition table. As a result, if the PC is booted from a DOS system disk, the hard disk will be inaccessible.

It infects 720Kb and 1.44Mb floppy disks. On 1.44Mb floppies the original boot sector is re-located to cylinder 0, head 1, sector 15; this copy is not stealthed.

On May 23 and December 26 the virus attempts to overwrite the CMOS memory. There is a bug which will allow the virus to corrupt a maximum of only one CMOS byte.

Infected sectors contain the string **`FIND_ME!`** in the OEM field (at offset 3 in the sector), which gives the virus its name.

For self-recognition, the virus uses bytes 01, 46 at offset 2 in the sector (46 is F, the first letter of **`FIND_ME!`**).

Copyright © Dr Solomon's Software

Finnish.357

Type
Memory resident file virus.

Affects
COM files.

File Growth
357 bytes.

Description
The virus intercepts only the Exec. (4bh) function of interrupt 21.

Infected files all start with byte 93h (instruction XCHG BX,AX) and the virus uses this byte to check whether it has already infected a file.

Variants
378:
File growth is 378 bytes and infected files start with 90h.

709a-b:
File growth is 709 bytes and the virus uses F0.

Finnish Sprayer (Aija)

Type
Boot sector virus.

Affects
The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth
-

Description
Finnish Sprayer uses 1Kb of RAM and uses stealth to conceal itself when memory resident. It occupies 2 sectors on the disk. On the hard disk, the original partition sector is relocated to the end of the active partition.

The virus uses Ai at offset 45h in the boot sector for self-recognition.

The payload is to overwrite the hard disk with the contents of the interrupt vector table, on the 25 March. It displays the following string and then hangs the machine:

 Copyright © Dr Solomon's Software

FINNISH_SPRAYER.1. Send your Painting +358-0-4322019 (FAX), [Aija]

The following string in the virus is never displayed:

Tks to B.B., Z-VirX .....

Fish6 (Fish)

Type

Memory resident file virus.

Affects

COM and EXE files on any file access. COMMAND.COM is infected first.

File Growth

3,584 bytes. When the virus is memory resident, it uses stealth to conceal the increase in file size of infected files.

Description

Fish encrypts itself in memory in an attempt to conceal itself from scanners. This makes the PC run so slowly that the presence of the virus becomes apparent to the naked eye.

Fish adds 100 years to the file date as a self-recognition (DOS displays only the last two digits, so this change is not noticeable, and any program requesting the date is given the original date). The virus also preserves the original file attributes.

The virus also slows down any access to DOS, because of the many things it does whenever interrupt 21h is called. For example, *Fish* attempts to avoid detection in memory by encrypting itself between DOS calls, using a different key each time (the decryption routine, however, remains un-encrypted).

If the DOS date is 1991 or later, and an infected COM program is run, the virus announces itself with the message **FISH VIRUS #6 - EACH DIFF - BONN 2/90 '~knzyvo}'** and hangs the PC with a HALT instruction. (**NOTE:** This will be the second infected program run as *Fish* must be resident when the COM program is run. The first infected program run will load *Fish* into memory.) Any PC with the date set correctly will therefore find it spontaneously.

There are a number of side-effects, including slow running and wasted disk space because of growing files.

If 42 is subtracted from each of the ASCII values of the '**~knzyvo}** string, and the new values are converted back to text, this string becomes **tadpoles**.

Copyright © Dr Solomon's Software

Each file infection is encrypted with a different key so that each appears different.

Variants

The message implies that at least five other variants exist, but none have been seen or reported.

IMPORTANT: Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS disk, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will NOT be detected by a scanner which fails to detect the virus in memory and which scans the files with the virus active in memory. For this reason, Dr Solomon's strongly recommends that the Anti-Virus Toolkit programs are run from the original write-protected floppy disk until the virus has been removed. FindVirus will find *Fish* in memory, as a safety measure.

Flash (Blink)

Type

Memory resident file virus.

Affects

COM files between 1,000 and 64,303 bytes, and EXE files, on execution.

File Growth

688 bytes.

Description

At any time after June 1990, seven minutes after the virus goes memory resident it blinks the screen display four times and repeats this every seven minutes. If you single-step through the virus code it re-boots instead of running. This happens because when the virus patches the code (just a few bytes past the execution pointer), that patch is ignored since the CPU chip has already read the code.

Flip (Omicron, Omicron 2)

Type

Multipartite.

Affects

COM and EXE files on execution. COM files must be less than 62,857 bytes.

 Copyright © Dr Solomon's Software

File Growth

2,343 bytes. EXE files vary slightly.

If COMMAND.COM has been infected, the increases are hidden.

Description

Flip infects the partition sector when an infected COM or EXE file is run. The virus shortens the first partition by six sectors, using these sectors to store its own code and the original partition sector. The text string:

```
OMICRON by PsychoBlast
```

can be seen in one of these sectors. *Flip* was written when there was a 32Mb size limit for DOS partitions. The virus patches the Maximum Logical Sector (LSN) entry in the boot sector's BIOS Parameter Block (BPB) when subtracting six sectors from the partition.

You should not use FDISK /MBR to clean the partition sector, since the BPB will not be changed back and the drive will subsequently appear to be 32Mb. If DOS finds anything other than 0 for the first Maximum LSN number, it does not look at the second entry (introduced when the 32Mb size limit was exceeded), which contains information on the real size of the partition. On the second of each month at 10.00am, on PS/2s or ATs, EGA and VGA screens are reversed.

Variants

2343.a, 2343.b, 2153.a.

Form (Form 18, Form May)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

On hard disks, the virus copies the original boot sector to the last sector of the physical disk. The second sector of the virus is copied to the second last sector of the physical disk. This sector contains the text (which is not displayed):

```
The FORM-Virus sends greetings to everyone who's reading this
```

Copyright © Dr Solomon's Software

text. Form doesn't destroy data! Don't panic! Fuckings go to Corinne.

On floppy disks, the virus creates 1Kb in fake bad sectors, which is used to store the original boot sector and its own code. These bad sectors are reported by CHKDSK.

On the 18th of each month, the PC is supposed to click when a key is pressed. This will not happen if any program, loaded after the virus goes memory resident, traps keyboard input (for example, KEYB).

Variants

Form.a, Form.b and **Form.e**. In the case of **Form.e**, the text **STIR** replaces the above message.

Frankenstein (Frank, SBlank)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus has a memory resident infection system. It has intermediate stealth capability. The whole virus is encrypted. The virus overwrites infected files.

Freddy

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

The virus has a special routine which infects COMMAND.COM, increasing its size by only 77 bytes

 Copyright © Dr Solomon's Software

Description

Self-recognition is interrupt 21 with AH=FF. The correct response is AH=FE.

When activated, the virus re-writes the boot sector using interrupt 25 with the string **`FREDDY KRG 0.`** The PC hangs and will not boot afterwards.

To store itself in memory, the virus uses a legal DOS call to set a memory block (4A).

Variants

1870, 1878.

Frodo (Century, 4K, 4096, IDF, Hidden, 100 Years)

Type

Memory resident file virus.

Affects

COM and EXE files on almost any operation.

File Growth

4,096 bytes. When the virus is memory resident, it uses stealth to conceal the increase in file size of infected files.

Description

Frodo goes memory resident when an infected program is run. It then infects COM and EXE files on almost any operation. *Frodo* adds 100 years to the file date as a self recognition (DOS displays only the last two digits, so this change is not noticeable; and any program requesting the date is given the original date). The virus also preserves the original file attributes.

If the file is memory resident, it uses stealth to conceal the increase in file size of infected files.

NOTE: There is a code in the virus which is intended to install a routine on the partition sector of the hard disk and the boot sector of any disk in drive A. When the PC is booted, it is designed to display **`FRODO LIVES`** in large block graphics with a surrounding flashing neon border. This is designed to happen between September 22nd and December 31st. However, the routine designed to do this is corrupted and the PC hangs when the routine is called.

Variants

Frodo.a:

Copyright © Dr Solomon's Software

Frodo-b:
Replicates as above, but if it did the partition drop (which still does not work), the dropped partition record would not work as several bytes have been nulled out.

IMPORTANT: Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS disk, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will NOT be detected by a scanner which fails to detect the virus in memory and which scans the files with the virus active in memory. For this reason, Dr Solomon's strongly recommends that the Anti-Virus Toolkit programs are run from the original write-protected floppy disk until the virus has been removed. FindVirus will find *Frodo* in memory, as a safety measure.

Frogs

Type
File virus.

Affects
A COM file on execution of an infected file.

File Growth
1,500 bytes.

Description
On the 5th of each month, when an infected program is run the virus displays the message **`(V) AIDS R.2A - Welcome to Frog's Alley!, (c) STPII Laboratory - Jan 1990`** after exiting. It also deletes the first file in the current sub-directory.

Fu Manchu (2086)

Type
Memory resident file virus.

Affects
COM and EXE files on execution, except COMMAND.COM.

File Growth
2,086 bytes. EXE files grow by 2,080 to 2,095 bytes.

 Copyright © Dr Solomon's Software

Description

When a warm boot is performed, the message **`The world will hear from me again!`** is displayed. If the date is after August 1st 1989, the virus monitors the keyboard buffer. If '**`Fu Manchu`**' is typed, the virus types back **`Fu Manchu virus 3/10/88 - latest in the new fun line!.`** If the name '**`Thatcher`**', '**`Reagan`**', '**`Waldheim`**' or '**`Botha`**' are typed, it adds in '**`xxxx`**' which is one of four obscenities. If either of the two most common English four-letter swear words are typed, it backspaces over them. The PC will also be re-booted at random intervals. The virus creates a TSR to perform these effects, taking 2Kb of memory.

This virus appears to be a re-write of ***Jerusalem***.

Fumble (Typo, Typo Com)

Type

File virus.

Affects

All COM files in the sub-directory on execution of an infected COM file. Infection only takes place on even dates. Date/time and read/write attributes are preserved.

File Growth

712 to 867 bytes.

Description

The DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is not disabled, so it is displayed when an attempt is made to infect a write-protected disk.

The virus occasionally replaces the letter typed with that of the key immediately to the right using the following table:

'1234567890-=\~!@#$%^&*()_+
|qwertyuiop[]asdfghjkl;'zxcvbnm,./
QWERTYUIOP{}ASDFGHJKL:";
ZXCVBNM?

The fumble only activates if you type faster than 60wpm. If you type at that speed, you get a fumble if the keyboard is untouched for five seconds. There is code in the virus which should gradually decrease the gap but it does not work correctly.

Copyright © Dr Solomon's Software

Variants

Fumble.b:
Files grow by 755 bytes.

Fumble.c and **d** are minor variants.

Galicia (Spanish-Telecom-3, Kampana.mp.d)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This virus is encrypted, but with a constant key (XOR with FFFF which is equivalent to a NOT operation, when all bits are reversed).

For self-recognition, the virus uses the string V1 at offset 1b3 in the infected sector.

If a disk read is made on 22 May at 12:00am, the virus displays the message:

```
Galicia contra telefonica!
```

It then tries to format the first 255 sectors of the hard disk; but this format command (AX=05FF/Int_13h) is not recognised by IDE and SCSI drives (it can only affect some old MFM HDDs); so the virus generally fails miserably to do any damage.

GENB

Type

-

Affects

-

File growth

-

 Copyright © Dr Solomon's Software

Description

This is a name used by McAfee's Scan program when it suspects that the boot sector is infected but cannot identify which virus has caused the infection. McAfee use this shorthand to mean "Generic boot sector virus". Running Dr. Solomon's will normally tell you the specific name of the virus.

GENP

Type

-

Affects

-

File Growth

-

Description

This is a name used by McAfee's Scan program when it suspects that the partition sector is infected but cannot identify which virus has caused the infection. McAfee use this shorthand to mean "Generic partition sector virus". Running Dr. Solomon's will normally tell you the specific name of the virus.

Gergana

Type

File virus.

Affects

A COM file in the current directory on execution of an infected file.

File Growth

182 bytes.

Description

The text **`Gergana`** can be found in the virus.

Copyright © Dr Solomon's Software

Ghostballs (Ghost)

Type
File virus.

Affects
COM files on execution, including COMMAND.COM. File attributes are preserved. The Critical Error Handler is not disabled, so any attempt to infect a write-protected floppy disk will still display the usual message.

File Growth
2,351 bytes.

Description
The code contains the message:

```
Ghostballs, Product of Iceland

Copyright (c) 1989, 4418 and 5F19
```

which is never displayed.

When an infected application is run, the virus tries to read the boot sector of the disk in drive A. If this attempt is successful, it drops a copy of ***Big Italian*** (with all infective code removed) on to the boot sector.

Ginger (Gingerbread)

Type
Multipartite virus.

Affects
COM and EXE files and partition sectors.

File Growth
See Variants.

Description
When an infected COM file is run, *Ginger* infects the partition sector. When the PC is next booted, the virus goes memory resident and infects any COM file which is run.

The virus uses the five sectors immediately after the partition sector (sectors 2, 3, 4, 5 and 6) to store its own code. The following text can be seen in sector 2:

```
You can't catch the Gingerbread man. .

Bad Seed . . . made in OZ
```


Copyright © Dr Solomon's Software

Ginger modifies the partition table so that, instead of passing control to cylinder 0, head 1, sector 1 (the DOS boot sector), it points to cylinder 0, head 0, sector 2 (virus code), which then passes control to cylinder 0, head 1, sector 1.

When the virus is memory resident, it uses stealth to conceal itself. If the partition sector is examined in a 'dirty' machine (that is with the virus active in memory), the virus displays the original, clean partition sector.

If you attempt to boot the PC from a DOS system disk, versions 4.x, 5.x or 6.x, DOS is unable to handle the fact that the partition sector code points back to itself. The result is that the PC fails to boot. A PC infected with this virus should be booted from DOS 3.3, Novell DOS 7 or Dr Solomon's Magic Bullet.

Variants

2691, 2774, 2848.

Ginger.Orsam.2620 and Ginger.Orsam.2624:
As for *Ginger,* but with one important difference. The virus alters the partition sector so that, instead of pointing to cylinder 0, head 0, sector 2 (the virus), which then points to cylinder 0, head 1, sector 1 (the boot sector), it executes the code in cylinder 0, head 0, sector 1 (the partition sector), points back to that code, AND ONLY THEN points to cylinder 0, head 0, sector 2 and cylinder 0, head 1, sector 1.

GoldBug

Type

Multipartite virus.

Affects

EXE files, the partition sector of the hard disk and the boot sector of 1.2Mb floppy disks.

File Growth

-

Description

GoldBug is polymorphic and uses stealth to conceal itself when memory resident. It infects EXE files using the companion technique. The virus intercepts interrupts 13h and 21h.

The infected partition sector always starts with **`CHKLIST????`** which appears to be a legal sequence of processor commands (INC, DEC, PUSH and AAS). On floppy disks, the body of the virus is written to two unused sectors (the virus checks to see if these sectors are really free).

Copyright © Dr Solomon's Software

The virus does not work on XT machines, because it hides the body of the virus in HMA memory (created by the HIMEM.SYS driver). During the boot process, the virus hides itself temporarily in video memory (it does this because HIMEM.SYS is not yet loaded and, as a result, HMA memory is not present).

Goldbug attacks anti-virus software named *AN.* and *AV.*. It also deletes CHKLIST.* files.

The virus has a payload. It instructs the modem (if present) to answer incoming calls on the 7th ring and continue work with the line (this is done with the command **ATMLS0=701**).

When Microsoft Windows is loaded on an infected machine, the virus 'disinfects' the partition sector; and re-infects it again when the Windows session is finished.

Goldbug contains the following strings:

```
107=0SLMTA
```

```
CHKLIST????
```

Variants

a-f.

Good Times

Type

Hoax.

Affects

-

File Growth

-

Description

Good Times is not a virus but a hoax instead.

GP1 (Jeru-GP1)

Type

Memory resident file virus.

 Copyright © Dr Solomon's Software

Affects
Executable files on execution, but only when IPX (part of the Novell Netware shell) is loaded. Only files between 4 and 64,496 bytes are infected.

File Growth
COM: 1,813 to 1,845 bytes.
EXE: 1,526 to 1,573 bytes.

Description
The text **`GP1 Removed from memory`** can be found in the virus.

This is intended to be a demonstration of how to steal login passwords using IPX calls. Because of a number of bugs it does not work.

This virus is closely related to *Jerusalem*.

Variants
There is also a version where the password stealing routine works.

Greemlin (Diamond-Greemlin)

Type
Memory resident file virus.

Affects
COM files (between 1,146 and 63,878 bytes) and EXE files (greater than 1,164 bytes) on execution.

File Growth
1,146 bytes.

Description
The text **`greemlin`** can be found in the virus.

If an infected EXE file is run on June 14th, the virus trashes the first six sectors of the first three floppy disks. If it is a Tuesday it trashes the first six sectors of cylinder 4, head 0 of drive A. A screen display can be triggered at any time.

Green Caterpillar (Find, 1591, 1575)

Type
Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files when a directory is examined. The next uninfected executable file in that directory is infected. This virus works only on an AT or PS/2 with a CMOS clock.

File Growth

COM: 1,583 to 1,591 bytes.
EXE: as COM, but may vary slightly.

Description

At any time after two months from the date of infection, provided the screen is not mono MDA, the caterpillar is triggered. The caterpillar has a green body, a yellow head and a red mouth. It starts at the top left of the screen and works its way across, line by line from top to bottom. It takes characters and drops them out of its rear end, displaced by 10 characters to the left and converted to yellow on black.

Variants

a, b, c.

GreenStripe

Type

Macro virus.

Affects

Lotus AmiPro documents by use of Word macros.

File Growth

-

Description

This virus infects AmiPro document files (*.SAM) by creating, for every SAM file, a corresponding SMM file (AmiPro macro) file with the same name in the same directory, and linking SAM to SMM files in such a way that opening the SAM file invokes execution of the SMM. SMM files are hidden and cannot be seen with a simple DIR command (however, DIR/AH will work).

When an infected document is opened, the virus gets control and infects all *.SAM files in the current directory, which is always AmiPro's default DOCS directory (...\AMIPRO\DOCS). The process is very noticeable, since all the document files are opened and then closed one by one; and you can see them quickly appearing/disappearing on the screen.

 Copyright © Dr Solomon's Software

Then the virus intercepts File/Save and File/Save As commands. On File/Save As the virus infects the document being saved. This is the only way the virus can propagate to another computer. Both SAM and SMM files are necessary for the virus. However, since the SAM file contains an absolute pathname as a reference to the appropriate SMM file, if you simply copy either the SAM file or both the SAM and SMM files to a floppy disk and then open SAM under AmiPro on a different PC, the virus will not run. But when a document (SAM) is copied using File/Save As, both SAM and SMM are transferred and the pathname link is changed accordingly.

File/Save was supposed to be used for the payload of the virus. On File/Save the virus should replace all occurrences of '**its**' in the document with '**it's**'. However, this does not appear to work.

Unlike Word macro viruses, ***AMP.GreenStripe*** is very unlikely to be transmitted by e-mail. Again, this is due to the fact that AmiPro keeps macros in separate SMM files, while only the SAM file is sent as an e-mail attachment.

The name of the virus - ***AMP.GreenStripe*** - is taken from the virus itself. Its main macro procedure is called Green_Stripe_virus.

Detection is made easier by a number of factors:

1. When an infected document is opened it is very noticeable - the screen keeps blinking as numerous documents are loaded and then closed.
2. After loading a document, you can use Tools/Macros/Edit to check whether the document has an appropriate macro file (same name, SMM) assigned to it to be executed on open.

   The report will contain the names of all infected (and now deleted) SMM files. Then you should run Ami Pro and for each SMM file listed in the report load the SAM file with the same name. There will be an error message (indicating that the appropriate SMM file was not found). Then you can use Tools/Macros/Edit and uncheck the Assign box(es).

Grower-268 (V270X)

Type

File virus.

Affects

The next uninfected COM file on execution of an infected file.

Copyright © Dr Solomon's Software

File Growth

Each generation is one byte greater than the last, so the growth is equal to, or greater than, 268 bytes.

Description

The virus is encrypted.

Guppy

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

152 bytes.

Description

There is no payload.

Hahagif

Type

Companion virus.

Affects

COM and EXE files.

File Growth

-

Description

When a COM or EXE program is run, the virus renames the original (clean) file, for example, from PROG.COM to PROV.VOM. It also sets the attribute for this file to 'hidden'. Then the virus creates a new (infected) file with the original name, but 681 bytes longer.

If you boot 'dirty' (that is, with the virus in memory), you see normal filenames and the virus stealths to prevent the additional 681 bytes being seen.

Copyright © Dr Solomon's Software

If you boot clean, you see the true length of the infected file, but because of the 'hidden' attribute you do NOT see the original, renamed file.

Hallöchen (Hello 1a)

Type

Memory resident file virus.

Affects

Uninfected COM and EXE files on execution, unless dated the current month. COM files less than 5,000 bytes and greater than 63,510 bytes. There is also a test for EXE files (greater than 5,000 bytes and less than 64Kb), but they all pass. Read/write and date/time attributes are preserved.

File Growth

2,012 to 2,027 bytes.

Description

This virus was found in Germany, so the messages are in German: **`Hallöchen !!!!!!, Here I'm`** and **`Acrivate Level 1`**. These are not displayed.

After 50 infections the machine gradually slows down. If the number of infections is greater than 70, it adds a keyboard handler in which 70 is subtracted from the infection count and the result divided by 2. This then becomes the number of chances out of 256 for any given keystroke to be corrupted. The corruption consists of 1 being added to the ASCII value for all values over 32, so A becomes B, B becomes C and so on.

Harakiri (HLLO.Harakiri)

Type

Overwriting file virus.

Affects

-

File Growth

-

Copyright © Dr Solomon's Software

Description

This virus is an old (1992), unremarkable high-level language virus. The virus was written in Pascal and simply overwrites files with itself.

Variants

There are two slightly different variants.

Hare.7610 (Krsna, Hari, HDEuthanasia)

Type

Multipartite virus.

Affects

COM and EXE files.

File Growth

7630 and 7800 bytes.

Description

Hare.7610 is a virus which has been reported repeatedly in many countries around the world (United States, Canada, UK, Switzerland, Russia).

Hare.7610 is a multipartite, stealth, slow polymorphic virus. It is memory resident and infects COM and EXE files on execution. The virus also infects the partition sector of the hard disk and the boot sector of floppy disks. Infected files grow in size between 7630 bytes (approximately) to 7800 bytes (approximately).

The virus overwrites the partition table in the partition sector. When the PC is booted from a clean system disk, the hard disk is inaccessible at a DOS level. Access is normal when the PC is booted from the hard disk.

The virus triggers on 22 August and 22 September, displaying the message:

```
"HDEuthanasia" by Demon Emperor: Hare Krsna, hare, hare...
```

and overwriting all hard disks in the system, destroying all data on them.

Hate (Klaeren)

Type

Memory resident file virus.

 Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution, except COMMAND.COM and COM files greater than 63,852 bytes.

File Growth

978 to 1,000 bytes.

Description

The virus is encrypted.

In May 1991 the virus trashes the CMOS and displays the message:

`Klaeren Haß, Haß!`.

There is some relationship with ***Jerusalem***.

Headcrash

Type

Memory resident file virus.

Affects

The next COM file in the directory on execution of a program. Files must be between 1,792 and 61,696 bytes, and the current day must be an odd-numbered day.

File Growth

1,067 bytes.

Description

On odd-numbered days, if a program is loaded in a 5-minute window in each hour, the message **`Headcrash Industries celebrate 0054 hex`** is displayed, where 0054 is replaced by a counter of the number of programs run. The 5-minute window is variable depending on the instance of the virus.

Helloween (1376)

Type

Memory resident file virus.

Affects

COM and EXE files.

Copyright © Dr Solomon's Software

File Growth

-

Description

The virus has a memory resident payload and infection system. It has minimum stealth capability. Some messages in the virus are encrypted. The virus evades or attacks some anti-virus programs.

Variants

1182, 1376.a-f

Variant **1182** has an ineffective length of 1,182 bytes and occupies 1,696 bytes in memory. Variant **1376** has an ineffective length of 1,376 bytes and occupies 1,904 bytes in memory.

Normal stealth is used, so that, for example, the date and time of infected files is preserved.

The virus looks for files containing the following and, if it finds them, does not infect them:

SCAN, SHIE, TRAP, VIRU, VCOP, ASTA, ALIK, AZOR, REX. MAND, VEXE, VCOM, VIRI, CLEA, TSAF, NAV.INI, BOOT.

In doing this, it aims to avoid infecting some anti-virus programs, which perform an integrity self-check.

A message is displayed, on ATs only, with either color or mono monitors (on color monitors the message is in white on a red background):

```
Nesedte porad upocitace a zkuste jednou delat neco rozumenhol!
                    ******************
 !!Poslouchejte HELLOWEEN - nejlepsi metalovou skupinu!!
```

The **1376** variant displays this message on November 1st. The **1182** variant, which is the more common of the two, captures interrupt 21h (DOS functions), interrupt 8 (the timer tick) and interrupt 13 (floppy and hard disk access). When the timer tick reaches 0, it causes an occasional time-out so that accesses to floppy disks fail to work.

1227, 1228, 1288, 1384, 1401, 1447, 1839, 1888.

 Copyright © Dr Solomon's Software

Hero (Siskin-Hero-506)

Type

Memory resident file virus.

Affects

COM files on execution. Files can be re-infected.

File Growth

506 bytes.

Description

The virus uses the upper half of the interrupt vector table for storage.

On the first day of the month a message is displayed. This is encrypted in the file and the decryption does not appear to work as the displayed message is blank.

Hidenowt.1741

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

1,741 bytes.

Description

Hidenowt is partially-encrypted and uses anti-tracing tricks.

The virus intercepts INT_21 and INT_24 and infects on findfirst and findnext functions. For self-recognition of infected files, the virus uses the marker 59 78 (Yx) near the file end (at offset end of file -6).

Hidenowt always tries to infect COMMAND.COM. It does not infect programs if the checksum of the name coincides with one of five 16-bit values.

HLLC.Even_Beeper

Type

-

Copyright © Dr Solomon's Software

Affects

-

File Growth

-

Description

The virus is not memory resident. It has no stealth capability and is very visible. The virus is not encrypted. The virus plays music or beeps.

Variants

a-d.

Horse (Hacker, Naughty Hacker)

Type

Memory resident file virus.

Affects

COM and EXE files on execution and reading.

File Growth

1,154 bytes. The virus uses stealth to conceal the increase in file size.

Description

The text **`Sofia,Jan 1991 (c) Naughty Hacker`** can be found in the virus.

When a counter reaches 0, a sound is made on the speaker and the screen displayed is interfered with, changing the horizontal synchronization to a new value. The counter is initialized to 13,398 and decremented each time DOS is called.

Variants

Horse 2 (Hacker 2):

Files grow by 1,160 bytes (Version **2b**) or 1,158 bytes (Version **2**). They are infected when they are run, closed or read, and the date in the text string is **`Feb '91`**. All effects are the same, except there is no sound.

Horse 3 (Hacker 3):

Files grow by 1,594 bytes (Version **3.1**) or 1,610 bytes (Version **3**). They are infected when they are opened, created, read, run, or when various other DOS functions are

 Copyright © Dr Solomon's Software

called. COMMAND.COM is avoided. If the virus is memory resident the growth is hidden from DIR and other programs checking file sizes. The strings **`Naughty Hacker`** or **`N. Hacker`** (Version **3.1**) can be found in the virus. Single-step tunneling is used to get under interrupts 13h, 21h and 2Fh. There are no other effects.

Horse 4 (Hacker 4):

Same as **Horse 3**, except that files grow by 1,776 bytes. Each time a DOS function call is made, a counter (initialized to 9,029) is decremented. At zero, a routine is installed on the timer tick which interferes with color screens.

Horse 5 (Hacker 5):

As **Horse 3**, but files grow by 1,576 bytes.

Horse 6 (Hacker 7):

As **Horse 3** except that files grow by 1,594 bytes. Disk-reads are occasionally converted to writes and vice-versa, when a file is closed.

Horse 7 (Hacker 7):

As **Horse 1**, except that the date in the text is changed to **`Jan.Feb 1991`**.

Horse Boot

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Floppy disks: The original boot sector is moved to cylinder 39, head 1, sector 9.

Hard disks: The original partition sector is moved from cylinder 0, head 0, sector 1 to cylinder 0, head 0, sector 7.

Copyright © Dr Solomon's Software

HLLO.Novademo (HLL.ow.12288, HLLO.Messanger)

Type

File Virus.

Affects

EXE files.

File Growth

-

Description

This is a high-level language, overwriting virus (that is, the virus overwrites code in the program being infected), apparently written in Pascal. The **a** and **c** variants are compressed with PKLite 1.15.

The **a** variant contains visible text in the EXE header, which gave the name to all these viruses:

```
Finish demogroup NOVA 1994!
```

Other messages are not visible, except for variant **b** (which is not compressed).

Messages in variant **a**:

```
This is Dangerous Messanger, and here is my message to the
world

Bad command or file name

Computer protected, no action.

Dangerous Messanger was here!

Can't initalize hardware... Try on another computer...

*.exe
```

Messages in variant **b**:

```
This is Dangerous Messanger, and here is my message to the
world v1.1

Bad command or file name

Computer protected, no action.

Dangerous Messanger was here!

Sound init fails.
```

 Copyright © Dr Solomon's Software

***.exe**

Messages in variant c:

This is Dangerous Messanger, and here is my message to the world v1.2

Bad command or file name

Computer protected, no action.

Disk error

Dangerous Messanger was here!

EMS page fault. Check EMS driver.

***.exe**

DOS ATTRIB function

Variants

a-c

Hungarian-482

Type

Memory resident file virus.

Affects

COM files on execution. Only files between 254 and 64,000 bytes are infected.

File Growth

482 bytes.

Description

On November 7th, if an infected program is run the message **Format ...** is displayed, and the virus writes rubbish progressively along the hard disk starting at the partition sector. It overwrites only head 0 and the first cylinder because of a bug.

Hybryd

Type

File virus.

Copyright © Dr Solomon's Software

Affects

COM files on execution of an infected file.

File Growth

1,306 bytes.

Description

The string **AKUKU** can be found in the code.

On, and after, Friday 13th 1992, the virus drops a trojan on to the boot sector of the current drive and trashes 1 file in 8 by patching the first five bytes. There is a 1-in-4 chance that it will set the number of floppy disk drives to 1 and the memory to 256Kb in the equipment byte.

The trojan first displays the message:

Wirus v. 1.0 (c) Hybryd Soft Specjalne podziekowania dla Andrzeja Kadlofa i Mariusza Deca za artykuly w Komtuterze 11/88

then it formats cylinder 10, head 0 of the drive and displays **Formatowanie zakonczone**.

This virus is a development of *Vienna*.

Hymn

Type

Memory resident file virus.

Affects

COM and EXE files of greater than 2,816 bytes on execution, opening, creation, closing, renaming, or change of attribute.

File Growth

1,865 to 1,977 bytes.

Description

The strings **.WV.** and **ussr** are found in the virus.

When the date equals the month (January 1st, February 2nd, and so on) the virus alters the boot sector, replacing the OEM label with IBM 3.3 and Russian music is played.

 Copyright © Dr Solomon's Software

Variants

Sverdlov:

Files grow by 1,962 bytes. The virus goes memory resident without using any DOS calls and the text string `.vs.` can be found in the virus.

Hymn-2144:

This is a larger version. When this triggers, it also nulls the BPB data in the boot sector. With some versions of DOS this means that the PC cannot be booted even from a DOS system disk. If this occurs, try booting from a different version of DOS. The PC may be booted from Dr Solomon's Magic Bullet.

Icelandic (Saratoga, Disk eater, Disk crunching)

Type

Memory resident file virus.

Affects

EXE files on execution (a counter set up and maintained by the virus means that every alternate file is infected). Date/time are not preserved. The resident part of the virus takes 2Kb of memory.

File Growth

632 to 647 bytes, depending on the version.

Description

The virus goes memory resident without using any DOS calls, so some detection software may not find it.

Every time a file is infected, the virus tries to mark a bad sector on the hard disk. Because of the way it does this, the attempt will fail until a certain number of files are infected. After that, the number of bad clusters will increase with the number of infected files.

Icelandic does its own memory management, so memory mappers and monitors may not detect it.

Variants

Icelandic 1-b:

Every tenth program is infected.

Copyright © Dr Solomon's Software

Icelandic 2:

This does not use interrupt 21h for file reading and writing, but searches for the relevant code, making a far call to the routine there. This is to defeat any anti-virus software which detects illegal writes to EXE or COM files by assuming that all file reads and writes go via interrupt 21h. This version does not mark bad clusters on the hard disk, but infects every tenth program.

December 24th:

A development of **Icelandic 2**. EXE files grow by between 848 and 863 bytes, and every tenth file is infected. If the virus goes memory resident on December 24th the message **`Gleôleg jòI`** is displayed instead of the program being run.

A big difference between this and the older *Icelandic* viruses is that the date/time is preserved and the DOS Critical Error Handler is disabled to avoid the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message. However, there is a bug in the code here and if there is a critical error the PC is likely to hang.

Incom

Type

File virus.

Affects

All COM files in the current sub-directory on execution of an infected file.

File Growth

648 bytes.

Description

The virus is encrypted.

There is a 10% chance that the color palette displayed on an EGA or VGA monitor will be changed.

Int13

Type

Memory resident file virus.

 Copyright © Dr Solomon's Software

Affects

Uninfected COM files on a directory request. It will only infect files of greater than 512 bytes and with not less than 512 bytes of slack space between the end of the file and the end of the cluster. Only files between 4 and 64,496 bytes are infected.

File Growth

None.

Description

The text **`Int 13`** can be found in the virus. The virus takes effect only with a color monitor. If the system has a mono monitor, the system will hang.

Internal (1381)

Type

File virus.

Affects

EXE files (chosen randomly) on execution of an infected file. The files infected depend on the contents of the header.

File Growth

1,381 to 1,467 bytes.

Description

If an infected file is run 90 days or more after the infection, the trojan is triggered. This consists of a letterfall followed by the message:

```
INTERNAL ERROR 02CH

PLEASE CONTACT YOUR HARDWARE MANUFACTURER IMMEDIATELY!

DO NOT FORGET TO REPORT THE ERROR CODE!
```

The infected file is then disinfected.

Variants

2C as above.There is also a version where the 2C in the message is replaced by 2E.

Copyright © Dr Solomon's Software

IR&MJ

Type

IR & MJ is a boot sector virus infecting 1.44 Mb and 720k floppies. The virus body is stored on track 0, sector 7 of the hard disk drive. On a 1.44MB floppy it is stored on head 1, sector F. On 720k disks it is stored at head 1, sector E.

Affects

-

File Growth

-

Description

On 30 December the virus displays: **" December 30th (C) by IR&MJ Compu Serve 1993"** and does not load into memory.

The virus does not stealth changes to the partition sector.

Istanbul

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

This virus infects COM and EXE files on execution. Both variants are written to avoid infecting COM files on 15 December 2000, if they start with anything except JMP (E9h).

To check for itself in memory, the virus issues a call, AX=4624/INT_21h; the correct response is AX=3434. The virus intercepts interrupt 24h, to suppress critical errors (for example, the DOS write-protect error message).

The messages in the two variants are, respectively:

Written in the city of Istanbul (c)1993. and **Installed**

Copyright © Dr Solomon's Software

Anti-Virus?? Written in the city of Istanbul (c)1993. and **Installed**

Variants

1312, 1349.

Itavir

Type

File virus.

Affects

The next uninfected EXE file in the current sub-directory on execution of an infected program.

File Growth

1,600 to 7,000 bytes.

Description

This virus reads and writes to the files without using interrupt 21h, by using interrupts 25h and 26h and decoding the FAT. This will evade TSR virus detectors.

If the number of the month is even, the date is the 21st and the time is 3 p.m, or after, the trojan is triggered. The keyboard is disabled and the following message is displayed:

.....AHI..AHI..AHI.....

Ho proprio l'impressione di essere un Virus Maligno.....

Molto maligno (maturalmente)

Non vi rimane che da azionare l'interruttore AUGUR!!!.....

Then all sectors of all logical drives are overwritten with garbage.

IVL (HIV-1)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution or opening. COM files must be between 1,614 and 64,000 bytes and EXE files must be between 1,614 bytes and 64 Kb.

File Growth

1,614 bytes.

Description

The string **`HIV Virus - Release 1.0 Created by Cracker Jack (C) 1991 Italian Virus Laboratory`** can be found in the virus.

Every Saturday the message is displayed each time an EXE program is run, instead of running the program. Between 4 p.m. and 5 p.m. the screen trick is triggered, which consists of a face character which bounces around the screen rather like *Ping Pong*.

This virus is in the same family as *Swami*.

Jabberwocky

Type

Memory resident file virus.

Affects

COM and EXE files on execution. EXE files are infected by conversion to the COM structure, so only files of 65,024 bytes or less are infected.

File Growth

812 bytes.

Description

The text **`JW2`** can be found near the start of the file.

Occasionally, when an infected program is run, it beeps and the message **`BEWARE THE JABBERWOCK`** is displayed.

Variants

A previous version, which only infected COM files, was not released by the author (according to the author). This is 615 bytes long.

 Copyright © Dr Solomon's Software

Jackal

Type

Multipartite virus.

Affects

Floppy and hard disks, and COM and EXE files.

File Growth

-

Description

The virus infects EXE files, COM files, boot sectors of floppy disks, and partition sectors of hard disks. It can survive a warm re-boot (Ctrl Alt Del), by intercepting the keypresses and 'faking' a re-boot.

Japanese Christmas

Type

File virus.

Affects

COM files on execution of an infected file.

File Growth

600 to 653 bytes.

Description

Every December 25th, the virus displays (in the centre of the screen) the message **`A merry christmas to you`**, cycling through the colors (green, yellow, blue, magenta, light blue, white, and so on) and blinking the characters as it goes.

Jeff (June 7)

Type

File virus.

Affects

COM files on execution of an infected file.

Copyright © Dr Solomon's Software

File Growth

Files are padded to a multiple of 16 bytes, then another 812 bytes are added.

Description

On the 7th of each month after June 1991, after infecting the next file the virus displays **`Jeff is visiting your harddisk...`**. Then it overwrites 126 sectors of drive C, starting with the first sector of the FAT, and hangs the PC.

Jerusalem (1244, 1808, 1813, Hebrew University, Israeli Mummy 2.1, Sunday, Friday 13th, Frère, Black Friday, Russian, Jerusalem-B, JV, Black Hole Morbus Waiblingen, sUMsDOS, Payday)

Type

Memory resident file virus.

Affects

COM and EXE files on execution, except COMMAND.COM.

File Growth

COM: 1,813 bytes. COM files are not re-infected. EXE: 1,808 to 1,823 bytes. EXE files grow each time they are infected until they are too large to load into memory. Some EXE files are infected, without growing, usually because the genuine EXE is followed by overlays in the same file. The virus uses 2Kb of memory. Occasionally an EXE is not infected correctly and fails to run as soon as it is infected.

Description

Every Friday 13th, when a program is run, it is deleted. On any date, 30 minutes after the virus has installed itself, a PC XT system slows down to a fifth of normal speed. On faster machines the slowdown is not as noticeable. At the same time, if the system is in text mode, a small black rectangle opens up, as the portion of the screen from row 5, column 5, to row 16, column 16, is scrolled up by two lines.

Jerusalem uses functions of interrupt 21h that Novell Netware requires, and so is incompatible with Novell Netware. Possible symptoms of this include workstations becoming disconnected from the network and the generation of large spool files.

 Copyright © Dr Solomon's Software

Variants

Jerusalem is the most common file virus, and because of this the code has been modified by a number of virus authors. The following are closely based on *Jerusalem*:

The Suriv viruses:

These are early, less sophisticated predecessors of *Jerusalem*. **Suriv 1** and **2** trigger on April 1st, **Suriv 3** triggers on Friday 13th. These viruses are not removable.

Sunday (Jeru-Sunday):

Files grow by approximately 1,636 bytes. Every Sunday, at approximately half-hourly intervals, the following text is supposed to be displayed:

```
Today is SunDay! Why do you work so hard?

All work and no play make you a dull boy!

Come on ! Let's go out and have some fun!
```

It is also supposed to delete every program as it is executed. However, there is a bug in the virus and neither the message display nor the file deletion work.

Sunday.a:

Sunday.b:

This is a working version of *Sunday*.

Sunday 1.b:

As for *Sunday*, but a bug in the Critical Error Handler, which causes a problem on write-protected disks, has been corrected.

Sunday 1.d:

As for *Sunday*, but a bug in the Critical Error Handler, which causes a problem on write-protected disks, has been corrected in a different way.

Sunday 1 Tenseconds:

As for *Sunday*, but the delay is 10 seconds and the test for Sunday has been corrected to day 0 (instead of day 7).

Sunday 2:

As for *Sunday*, but files grow by 1,733 bytes.

Anarkia:

Almost identical to *Jerusalem*, but uses the self-recognition code Arkia.

Copyright © Dr Solomon's Software

PSQR:

Files grow by approximately 1,720 bytes, and on the 13th of each month any program run is deleted. In addition, junk is written to the hard disk partition sector and the nine sectors after it. The self-recognition code is PSQR.

Jerspain (Jeru-Spanish):

On the 26th of each month, any program run is deleted.

Frère:

The virus plays Frère Jacques on Fridays and the 13th of each month.

Jerusalem-Westwood (Westwood):

Files grow by about 1,829 bytes, and on Friday 13th each file run is deleted.

Jerusalem-113b:

Programs will not run on any Saturday. COMMAND.COM is infected, and instead PHENOME.COM is avoided.

Jerusalem-Apocalypse:

The text **`Apocalypse!!!`** can be found in the virus, and the self-recognition code is C.J**. Every Friday 17th each file run is deleted.

Jerusalem-T1:

On Tuesday 1st, all files run are deleted.

Jerusalem-T13:

COM and EXE files grow by 1,812 bytes. It deletes programs executed on Tuesday 13th.

Jerusalem-Sat13:

Deletes programs executed on Saturday 13th.

Jerusalem-Czech:

On Friday 13th, the virus deletes each program run. Both the self-recognition and code placement are different from the original.

Jerusalem-Frère.2:

Once a minute the virus plays Frère Jacques. There is also a variant called **Two Tigers** which plays the same tune.

 Copyright © Dr Solomon's Software

Jerusalem-Nemesis:

Same as ***Jerusalem***, including Friday 13th deletion, but avoids infecting NEMESIS.COM instead of COMMAND.COM. It contains the string **`NEMESIS.COM`**.

Jerusalem-Captain Trip:

Contains the strings **`Captain Trips`** and **`SPITFIRE`**. If the year is not 1990 and it is a Friday on, or after, the 15th, every time a program is run an empty file is created with the same name. On other dates it installs a routine in the timer tick which triggers after 15 minutes. On June 16th it re-programs the video controller. The virus does not work properly.

Jerusalem-J:

COM files grow by 1,237 bytes and EXE files by 1,232 (after rounding to a multiple of 16). All ***Jerusalem*** effects have been removed.

Jerusalem-Yellow:

Files grow by 1,363 bytes. After 45 minutes, or after 4,096 keystrokes, a big yellow square with a shadow pops up in the centre of the screen and the PC hangs. This version does not repeatedly infect EXE files.

Jerusalem-Jan25:

Every January 25th, each program run is deleted.

Friday-15th (Skism):

Files grow by 1,813 bytes. On Friday 15th, the virus creates a file with the same name whenever a program is run.

Carfield (Jeru-Carfield):

Files grow by 1,508 bytes, and on Mondays every 42 seconds the string **`Carfield!`** is displayed.

Mendoza (Jerusalem Mendoza):

If the year is 1980 or 1989 it does nothing. Otherwise, when the virus goes memory resident, if the floppy disk drive motor count is 25, a flag is set. This will happen if the program is run from a floppy disk. If the flag is set, every program run is deleted. In years other than 1980 and 1989, if the delete flag is not set, 30 minutes after the virus is installed the cursor is changed from its current state to a block. After an hour, it switches **Ins, Caps Lock, Num Lock**, and **Scroll Lock** to Off.

Jerusalem.1244:

Jerusalem.1808.Standard:

Copyright © Dr Solomon's Software

Jerusalem.Mummy.1364.a:

Minor variants: **Standard.SuMsdos, Standard.Var, Standard.AA33CCDDEE, Standard.UMsDos, Standard.null, , Standard.Nocommand, Jan25, a, Anarkia.2, Puerto, Spanish, Messina, ffd, 1af, Critical, Flag_ee, *a204*, Frère2, Frère3, 2e7, Not13, b0f, Phenomen, 52f, 7c01, 6d46, JVT1, J, Friday15, 3503, Feb-7th, Nov30, sUMFDos, SKISM, 5a4, 65d6, BSA, Turkish,** and **Dragon**.

The name Friday 13th is not only applied to this virus, but also to two unrelated viruses: ***Friday 13th*** and ***Virus-B***.

Jimi (J&M, Jimmy)

Type

Boot sector virus.

Affects

The boot sector of 1.2Mb and 1.44Mb floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus is encrypted, using a simple XOR with a constant mask (FFh). It uses 2Kb of RAM; and partition sector disk-reads are not stealthed.

The original partition sector is re-located to cylinder 0, head 0, sector 6 of track 0. The virus occupies just 1 sector. The string **J&M**, after the encrypted virus code, serves as a virus marker; if the word at offset 1BBh is 264Ah (J&), this sector is considered to be infected. Infected partition sectors and boot sectors always start with EB 1C 90.

On floppy disks, the original boot sector is re-located to cylinder 0, head 1, sector 14 (the root directory, for 1.44Mb floppy disks).

On 15 November the **a** variant of the virus formats cylinder 0 of the hard disk using BIOS INT_13/AH=5. This will not work on SCSI, and most IDE, drives. The **b** variant triggers on 15 April.

Variants

a-b

 Copyright © Dr Solomon's Software

Jojo

Type

Memory resident file virus.

Affects

COM files on execution, including COMMAND.COM. It does not disable the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message when trying to infect a write-protected disk. It uses 2Kb of memory when memory resident.

File Growth

1,701 bytes.

Description

The text **`Welcome to the JOJO virus`** is near the beginning of the virus, and near the end is **`Fuck the system (c) - 1990 xxxxxxxxxxxxx zzz.`**

If an infected file is run after 7 p.m., it triggers a kaleidoscope display if run on a color screen. Mono systems simply hang.

This is a version of *Cascade* (the 1701 version), extensively hacked. The letter-fall code has been replaced by the kaleidoscope effect, and the encryption and decryption routines are not called.

Variants

Dazzler:

This is a harmless program which gives a dazzling screen effect. *Jojo*'s author used it as a sub-routine in *Jojo*. Some scanners search for that code, giving a false alarm on the harmless program.

Joker (Jocker, Wabik)

Type

Overwriting file virus.

Affects

EXE files on execution of an infected file.

File Growth

None.

Copyright © Dr Solomon's Software

Description

The virus copies itself to another file, overwriting it. Programs no longer work. The infected file must be called WABIK.EXE or it will not infect others.

Joker-01

Type

Memory resident file virus.

Affects

COM and EXE files on execution. Only infects COM files of less than 6,795 bytes and EXE files of less than 6,656 bytes.

File Growth

29,233 bytes, most of which is a bitmap of the display.

Description

The last eight bytes of infected files form the message **`JOKER-01.`**.

When the virus triggers, a full-screen animated picture of The Joker is displayed in color.

Joshi (Joshua)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Floppy disks: The virus replaces the boot sector and moves the original further up the disk. The boot sector of floppy disks is moved to a safe place, except on 720Kb disks where a bug in the virus causes it to write the body of the virus on to track 40.

 Copyright © Dr Solomon's Software

Hard disks: The virus moves the partition sector to cylinder 0, head 0, sector 9 and replaces it with its own code.

Every January 5th it saves the current screen to memory and replaces it with a display in 40-column mode in large type on a blue background with a double-line border, which says **Type `'Happy Birthday Joshi'!.`** This remains in place until the user types the text requested, then the original screen is restored.

July 13

Type

File virus.

Affects

An EXE file on execution of an infected file. Files with an EXE extension but no MZ signature (on the first two bytes) are deleted.

File Growth

1,201 bytes.

Description

On July 13th, it installs a screen changer on to the timer tick.

Jumper (French Boot, SillyBop, 2Kb, Neuville)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

If the PC is booted from an infected floppy disk, the virus goes memory resident and infects the partition sector of the hard disk. The virus infects any floppy disk which is accessed.

Copyright © Dr Solomon's Software

The virus copies the original partition sector to cylinder 0, head 0, sector 14. On floppy disks the original boot sector is copied to one of the root directory sectors.

Variants

There are two slightly different variants of the virus.

June 4 (Bloody)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

After 128 hard disk boots, and thereafter every 6, it displays **`Bloody! Jun.4, 1989`**.

360Kb disks: The boot sector is copied to cylinder 0, head 1, sector 3. This is the seventh directory sector, which is rarely used.

1.2Mb disks: The boot sector is copied to cylinder 0, head 1,sector 3. This is the third directory sector, and if it is in use a directory listing which starts OK ends up as gibberish.

Hard disks: The partition sector is copied to cylinder 0, head 0, sector 6.

This is based on ***Stoned***, but is very different.

June 16th (Pretoria)

Type

File virus.

Affects

All uninfected COM files on the current disk (or any COM file on the drive referred to in the command) on execution of an infected file. Date/time are preserved, but file attributes are not preserved. If the virus tries to infect a write-protected disk the DOS

 Copyright © Dr Solomon's Software

`Write protect error writing drive X: Abort, Retry, Ignore?` message is displayed.

File Growth

879 bytes, or to a minimum size of 1,758 bytes.

Description

This virus is very visible as it scans the whole directory tree looking for uninfected files to infect.

Every June 16th it scans through the root directory of the current drive, reading one sector at a time and converting any filename it finds to **ZAPPED**, with the attribute of a normal file. Thus sub-directories are no longer subdirectories.

Junkie

Type

Multipartite.

Affects

Partition sectors of hard disks, boot sectors of floppy disks, and COM files. This virus does not infect the boot sector of 360Kb floppy disks.

File Growth

Variable, between 1,027 and 1,041 bytes.

Description

The virus infects the partition sector of the hard disk when booted from an infected floppy disk. When the PC is re-booted, the virus goes memory resident and infects any floppy disk which is accessed and any COM file which is run.

If an infected COM file is run, the virus infects the partition sector and goes memory resident the next time the PC is re-booted.

This virus was the subject of much media hype when it was first discovered in Ann Arbor, Michigan. In truth there is little special about it. During infection, the virus disables the TSRs in the Microsoft and Central Point Anti-Virus products.

The virus only becomes memory resident on booting, not from executing an infected COM file. It is, however, a fast-infector, meaning that if the virus is not detected by an anti-virus scanner in memory it can be easily transferred to all COM files during a scan.

Copyright © Dr Solomon's Software

Justice

Type

Memory resident file virus.

Affects

DOS 3.1 and 3.30 only. COM files on execution, opening, renaming, or change of attribute. Files of greater than 64,272 bytes, and IBMBIO.COM, IBMDOS.COM and COMMAND.COM are not infected.

File Growth

1,242 bytes.

Description

The text **`...AND JUSTICE FOR ALL`** can be found in the virus.

Every time there is a disk write, a counter is incremented. If the write is to cylinder 0 (FAT or directory, depending on the geometry of the disk), the counter is reset to 0. If the counter reaches 246 the write is redirected to the cylinder one less than the target cylinder.

Kaczor.mp.4444

Type

Multipartite virus.

Affects

EXE files on foppy disks and the partition of the hard disk.

File Growth

4444 bytes

Description

This virus is polymorphic; and uses stealth to conceal itself when memory resident. It infects EXE files on floppy disks and the partition sector of hard disks when an infected EXE file is run.

The virus intercepts INT_12, INT_13, INT_1C and INT_21.

It is encrypted even in memory. When a particular section of virus code is needed, it is decrypted, executed and then encrypted again.

Copyright © Dr Solomon's Software

The word **kaczor** serves as a password. When it is typed-in at the keyboard, the virus cleans the partition sector and prints the message:

Zrobione

On a certain date the virus asks for a password; and the correct response is **pieck**.

On 3 March, *Kaczor* joggles the screen using the timer interrupt (INT_08).

Kamasya

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

1,098 bytes.

Description

The text **Kamasya nendriya prtir labho jiveta yavata jivasya tattva jijnasa nartho yas ceha karmabhih** can be found in the virus, and is displayed every Tuesday.

This virus is related to *Swami*.

Kampana-3445 (AntiTel, Telecom)

Type

Memory resident file virus, and partition sector virus dropper.

Affects

COM and EXE files on execution. A copy of *Telefonica* is dropped into the partition sector, and replicates in the usual way. It does not do this if *Stoned* is present.

File Growth

3,445 bytes but highly stealthed, and does not show for any of the five DOS calls giving the size.

Description

The virus uses stealth to conceal the increase in file size.

Copyright © Dr Solomon's Software

The message in the virus says **(C) 1990 Grupa HOLOKAUSTO (Barcelona, Spain) KampanaAnti-TELEFONICA: Mejor servicio, enores tarifas...** and is encrypted, as is the entire *Telefonica* code.

There is a relationship between this and both *Fish* and *Frodo*.

Variants

Kampana.a.

Kaos4

Type

File virus.

Affects

COM and EXE files in the current directory and in directories listed in the PATH. Infects one COM file and one EXE file on each invocation.

File Growth

697 bytes.

Description

The virus is direct action and not memory resident.

The virus contains the following strings:

[KAOS4 / Köhntark]

and

***.COM *.EXE PATH=** (which is encrypted using a NOT operation).

The virus has no INT_24 handler and produces the DOS message **Write protect error writing drive X: Abort, Retry, Ignore?** when trying to infect files on a write-protected floppy disk.

Variants

697.

Kemerovo (V257)

Type

File virus.

Copyright © Dr Solomon's Software

Affects

All COM files in the current sub-directory on execution of an infected file.

File Growth

257 bytes.

Description

Every time an infected file is run there is a 10% chance that the PC will re-boot.

Keydrop

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The text `(c) Copyright 1990 Keydrop inc.` can be found in the virus, and it uses 5Kb of memory.

Keypress (Twins, Turku, St Leos, 9.8min)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. If DOS 2 is running, files are also infected when they are read.

File Growth

1,232 to 1,487 bytes.

Description

Every 10 minutes, for a period of two seconds, the virus adds five more of the same key to any keypress.

Copyright © Dr Solomon's Software

Variants

a, b, c, d, e, Samsoft, and **1232.a. Samsoft** puts a message on the screen.

Keytrick

Type

Trojan.

Affects

-

File Growth

-

Description

Every 256th keystroke has a 1-in-4 chance of being ignored.

Kiev-483

Type

File virus.

Affects

COM files in the current sub-directory on execution of an infected file. Only files between 50 and 61,440 bytes are infected.

File Growth

483 bytes.

Description

The virus contains the string **`Kiev 1990`**.

Kitty

Type

Joke boot sector.

Affects

Boot sectors of floppy disks.

Copyright © Dr Solomon's Software

File Growth

-

Description

Booting from a floppy disk containing the joke causes a display of either **`We all love Kitty Bittersplit`** or **`Not a system disk (sorry)....`**

Kukac-Nagytud (Nagytud)

Type

Memory resident file virus.

Affects

COM files on opening.

File Growth

448 bytes.

Description

The text **`dv minden nagytud a naki Turbo @ ... ...`** can be found near the end of infected files.

This virus is similar to *Kukac Turbo*.

Kukac Turbo

Type

Memory resident file virus.

Affects

COM files on opening, if less than 65,204 bytes long.

File Growth

512 bytes.

Description

The string **`Turbo Kukac 9.9`** can be found in the virus.

If you press **PrtSc**, the above message is displayed repeatedly, resulting in a scrolling display.

Copyright © Dr Solomon's Software

Kylie (Jeru-Kylie)

Type

Memory resident file virus.

Affects

COM and EXE files on execution, except COMMAND.COM.

File Growth

2,272 to 2,287 bytes.

Description

The string **`Kylie Minogue`** can be found in the virus.

If a flag is set, the virus plays **`Never Too Late`**. However, there is nothing to set the flag.

This virus appears to be a re-write of *Jerusalem*.

Variants

There are two versions, one is slightly corrupted and hangs the PC when it tries to infect.

Lazy

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

720 bytes.

Description

The virus contains the text **`[ lazy ]`**.

The screen display slows down to a crawl. The virus always goes memory resident at 7000:A483, so if any other program uses that memory the PC will hang.

Copyright © Dr Solomon's Software

Leapfrog (V516)

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

516 bytes.

Description

This virus is unusual in that it does not patch the jump command at the beginning of the file. Instead, it patches the target of the jump. This makes it invisible to anti-virus programs which assume the jump is patched.

The DOS version is occasionally reported as zero.

Leech

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

1,024 bytes.

Description

The virus is slightly polymorphic and uses stealth to conceal the file size when memory resident. The virus contains the text **`The leech live ... April 1991 The Topler.`**

There is a 1-in-8 chance of seeing the message displayed and getting a 2-sector overwrite on the hard disk.

Lehigh

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COMMAND.COM on execution of a program, or when DOS searches for a file. The date/time is changed.

File Growth

None.

Description

The virus includes an infection counter which counts the number of times (not generations) the virus has replicated. When the virus replicates, the counter is set to 0, and each time it replicates it increments the counter, which is then written back to the COMMAND.COM on the current disk.

After the virus has copied itself four times, it corrupts the disk by writing code from the BIOS to sectors 1 to 32.

On a floppy disk it is difficult to recover from this damage, as both copies of the FAT and the directory will be overwritten. On most hard disks this will not extend as far as the second copy of the FAT or the root directory, so it is easy to recover from the damage.

After the overwrite, a string from the BIOS is displayed.

This was probably the first documented PC virus. It originated at Lehigh University in the USA and has never been found 'in the wild' outside the USA.

Variants

Another version has a counter of ten, and has not been found outside the USA.

Lemming (Keeper.Lemming)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

 Copyright © Dr Solomon's Software

Description

This virus uses stealth to conceal itself when memory resident. It is encrypted. COM and EXE files are infected when they are executed or closed.

The virus filters itself out of infected files when they are opened (this is to avoid detection by scanners, especially in heuristic analysis mode). The virus avoids infecting anti-virus programs from the following list:

```
TBAVTBSCANNAVVSAFEFPROT
```

The virus checks for itself in memory by issuing a call, AX=FFFE/INT_21; the correct response is AL=FF.

Lemming.2144 contains the following text:

```
TBDRV
SP You Will Never Trust Anti-Virus Software Again!!
ThunderByte-1994-Australia.        ver 1.0
[HiTMaN]
"!Packed file is corrupt"
```

Lemming.2160 contains the following text:

```
TBDRV
SP
The Rise and Fall of ThunderByte-1994-Australia.
You Will Never Trust Anti-Virus Software Again!!
[LEMMING] ver .99á
"!Packed file is corrupt"
```

Variants

2144, 2151,2160.

Leprosy

Type

Overwriting file virus.

Copyright © Dr Solomon's Software

Affects

An EXE file in the current sub-directory on execution of an infected file. Some variants can infect COM files. The virus overwrites the first 666 bytes of a file.

File Growth

-

Description

Overwritten programs no longer work.

There are two messages which may appear:

```
Program too big to fit in memory
```

or

```
NEWSFLASH! Your system has been infected with the incurable
decay of LEPROSY 1.00 a virus invented by PCM2 in June of 1990.
Good luck!
```

Variants

Leprosy-B:

The message is:

```
ATTENTION! Your PC has been afflicted with the incurable decay
that is the fate wrought by Leprosy Strain B, a virus employing
Cybernetic Mutation Technology(tm) and invented by T-PCM2 80.90
```

Leprosy-C:

When an infected program is run it infects the next EXE program in the current sub-directory, overwriting the first 321 bytes.

Leprosy-D:

This infects both COM and EXE files, overwriting the first 370 bytes. There are no messages.

There are also **e**, **f**, **g** and **h** variants, and **Leprosy.Busted**. The **h** variant says `This program requires Microsoft Windows.`

Leszoptad

Type

Boot sector virus.

 Copyright © Dr Solomon's Software

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Floppy disks: the boot sector is copied to cylinder 0, head 1,sector 3.

Hard disks: the partition sector is copied to cylinder 0, head 0, sector 6.
On the 255th generation, the virus displays **`leszoptad!`**.

Liberty

Type

Memory resident file virus.

Affects

An uninfected COM or EXE file on execution.

Date/time and read/write attributes are preserved. Some versions also act as a dropper, installing ***Liberty*** on boot sectors.

File Growth

COM: 2,858 to 2,868 bytes.
EXE: 2,858 to 2,888 bytes.

Description

The virus contains the string **`-MYSTIC-COPYRIGHT (C) 1989-2000, BY SsAsMsUsEsL`**. There is no payload.

Variants

Liberty.2857.a, Liberty.b, Liberty.c

Lisbon (648-Lisbon)

Type

File virus.

Copyright © Dr Solomon's Software

Affects

COM files in the current directory on execution of an infected file, except those less than 10 and greater than 64,000 bytes. The DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed when the virus attempts to infect write-protected floppy disks on access.

File Growth

648 bytes.

Description

The virus uses the seconds field of the directory to store an impossible value of 62 seconds.

One infection in four makes the file unusable. Eventually COMMAND.COM is infected, and then whenever the PC is started it hangs. It does this by putting the five characters **`@AIDS`** at the start of the file.

This virus is a variant of *Vienna*.

Variants

Lisbon.b:

One file in eight is patched instead of being infected. When that file is run the PC hangs.

Lisbon.c:

This does not replicate except from the original file.

Lisbon.d:

This does not patch other files.

Little Brother

Type

Memory resident file virus.

Affects

COM files.

File Growth

-

Copyright © Dr Solomon's Software

Description

The virus has a memory resident infection system. It has no stealth capability and is very visible. The virus is not encrypted. The virus deletes files.

Variants

276, 299, 300, 301, 307, 321, 349, 361a-b, 385.

Little Pieces

Type

Memory resident file virus.

Affects

EXE files on execution.

File Growth

1,374 bytes.

Description

Every 30 keystrokes the screen is cleared and the cursor placed at the top left-hand corner. After this has happened eight times the message **`One of these days I'm going to cut you into little pieces`** is displayed. This is encrypted in the virus. The counter for eight times is never reset. The effects are not enabled until after a file has been infected.

Little Red (Mao, Lred, Little Red Book)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

1,465 bytes.

Description

The virus attempts to infect COMMAND.COM immediately. This virus is a fast infector, infecting files on execution and directory access (functions 11h, 12h).

Copyright © Dr Solomon's Software

The virus intercepts DOS interrupt 21h. It uses stealth to conceal the size returned by the DOS functions 11h and 12h (findfirst and findnext), used by the DOS DIR command. However, command line shells (like Norton Commander) use different DOS functions (4Eh, 4Fh) and will report correct (non-stealthed) file sizes.

The virus has no destructive payload. The virus triggers on 9 September and 26 December (the birth and death dates of Mao-Tse Tung) and plays two melodies (apparently of Chinese origin).

Live after Death 1 (Phoenix 800)

Type

Memory resident file virus.

Affects

COM files on execution, except COMMAND.COM and those greater than 64,512 bytes. Some other file sizes are avoided, which means that approximately one file in eight is left alone.

File Growth

800 bytes.

Description

The string **`Live after Death`** is encrypted variably in the virus.

Interrupt 13h is modified so that if a verify is requested it always returns OK. If a write is requested and the flags are set to failure, a read is done instead of the write.

This virus is part of a long series from Bulgaria.

Live after Death 2 (V1226, Phoenix 1226)

Type

Memory resident file virus.

Affects

COM files on opening, except COMMAND.COM and those greater than 63,488 bytes. Some other file sizes are avoided, which means that approximately one file in eight is left alone.

 Copyright © Dr Solomon's Software

File Growth

1,226 bytes.

Description

The text is encrypted variably in the virus.

The FAT is gradually corrupted by occasionally swapping two entries while they are in the sector buffer. This means that anything monitoring disk writes will fail to see the corruption, as it happens in memory, and DOS does the write. In addition, at the interrupt 13h level some disk-reads are converted to writes.

This virus is part of a long series from Bulgaria.

Lovechild

Type

Memory resident file virus.

Affects

COM files on opening. The virus only works on MS-DOS 3.2. PC-DOS 3.2 systems hang.

File Growth

488 bytes.

Description

The text **`v2 (c) Flu Systems (R)`** can be found in the virus.

After 5,000 calls to interrupt 21h, when an EXE file is written there is a 75% probability that it will drop its trojan as a replacement. The trojan steps through the heads and cylinders of the hard disk, writing rubbish. It also displays the string **`LoveChild in reward for software sealing.`** The '**`sealing`**' is presumably meant to be '**`stealing`**'.

If you try to create a file, there is a 3-in-16 chance that you will create a sub-directory instead.

Lucifer (Diamond-Lucifer)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution.

File Growth

1,086 bytes.

Description

The virus uses stealth to conceal the increase in file size. There is a video display, and the message **`Lucifer (C) by C.J.`** is displayed on Tuesdays. The video display shows on color monitors exactly on each hour. A large multi-colored diamond appears in the centre which then shatters into smaller diamonds that bounce around the screen until it is completely clear.

This is one of the *Cracker Jack* viruses.

MacGyver (MCGY, Mac, MAC22, McGyv, Satan, Shoo, Jerus3)

Type

Memory resident file virus.

Affects

COM and EXE files (but see Description).

File Growth

See Variants.

Description

The virus uses stealth to conceal itself when memory resident

Variants **2803** and **2824** infect EXE files only. Other variants infect both COM and EXE files. Variant **4112** is multipartite; and infects the partition sector and boot sectors of floppy disks.

Variant **4112** avoids infecting the following anti-virus programs:

SCAN, ZLOCKE.

Copyright © Dr Solomon's Software

Virtually all viruses of this family contain similar text (in most viruses it is encrypted, except in **4480**). The text below is from **MacGyver.4645**:

```
  *MacGyver V3.0*
 Hi! I am MacGyver
  Written by
    Dark Slayer
in Keelung.  TAIWAN
Don't Worry.  I just
a Virus.  Ha..Ha...
```

The last box is displayed on the screen (using int_08h and accompanied by music in the 2803a-c variants) when the virus triggers. The trigger depends on the date and time.

Variants

2803 a-d, 2824, 3160, 4112, 4480, 4643, 4645.

Magnitogorsk

Type

Memory resident file virus.

Affects

COM and EXE files on execution. COM files must be between 2,560 and 62,976 bytes and EXE files must be greater than 2,560 bytes.

File Growth

2,048 to 2,560 bytes.

Description

If the virus is in memory, every time a program file is opened it is disinfected.

Once an hour the following message is displayed:

```
Mr. Lozinsky ! Just read documentation on your AIDSTEST (1-Oct-
90 version) we release new virus. Create improved versions of
```

Copyright © Dr Solomon's Software

AIDSTEST to use it for out future designes, please !
Magnitogorsk, 3-Nov-90

Variants

Magnitogorsk-2048:

Files grow by 2,048 bytes. Thirty-six minutes after going memory resident the screen is inverted unless it is a mono- character screen.

Major

Type

Memory resident file virus.

Affects

EXE files.

File Growth

See variants.

Description

EXE files are infected on execution. The virus is encrypted, but not polymorphic.

The virus uses around 30Kb of RAM. It intercepts interrupt 21h (DOS) and 08h (timer). Infected files are marked with the word **DEAD**, at offset 12h in the EXE header.

The virus triggers at night (2.00am); if the PC is not busy, the virus tries to patch the file \BBSV6\BBSUSR.DAT. Variant **1692** also tries to patch the files \BBSV6\BBSAUDIT.DAT.

The following strings are contained within variants **1644** and **1692**, respectively:

The Major BBS Virus created by Major tomwn to DOS

The Major Virus created by Weed and dedicated to

the Quantum BBS in Calgary, AB service users

Both variants contain some names, which are apparently some BBS's aliases (like Santa, Cindy, Herman, Minion, Puppet, Gnat, Image).

Variants

1644, 1692

 Copyright © Dr Solomon's Software

Maltese Amoeba (Irish, Grain of Sand)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. COM files must be between 450 and 63,000 bytes.

File Growth

2,498 to 2,565 bytes.

Description

The virus is polymorphic so is difficult for a scanner to detect. The following poem is encrypted within the virus:

```
To see a world in a grain of sand,
And a heaven in a flower
Hold infinity in the palm of your hand
And Eternity in an hour.
THE VIRUS 16/3/91
```

The following text is also included:

```
AMOEBA virus by the Hacker Twins (C) 1991 This is nothing, wait
for the release of AMOEBA II-The universal infector, hidden to
any eye but ours! Dedicated to the University of Malta- the
worst educational system in the universe, and the destroyer of
5X2 years of human life.
```

On November 1st and March 15th the trojan is triggered on ATs and above. This overwrites the first four sectors, starting from cylinder 0, head 0, sector 1, and repeats this for cylinders 1 to 29. This is repeated on all floppy disk drives. The next time the PC is started the poem is displayed.

Mange Tout (1099)

Type

Memory resident file virus.

Affects

COM and EXE files.

Copyright © Dr Solomon's Software

File Growth

1,099 to 1,115 bytes.

Description

This virus goes memory resident in the 'Twixt' region of memory (above DOS memory but below the top of BIOS memory) by shrinking the last DOS MCB to make room for it. It does not have any stealth mechanism so the file growth is easily visible.

When it goes memory resident it intercepts three vectors; 8 (System Timer), 9 (Keyboard Data Ready) and 21h (DOS services). INT's 8 and 9 are used for the trigger routine and INT 21h is used for infection.

Most of the virus in memory is encrypted, only being decrypted when in use. The code is decrypted to a location in the DOS data segment starting at address 00540h and is executed from that point. This is true of the INT 21h interceptor, the initial residency code and the payload routine. All the time that the code is decrypted, the keyboard is disabled by turning off the keyboard interrupt (IRQ 2) in the 8259A interrupt controller. After use, the code is overwritten with the words of 0CBBAh so it is no longer visible.

The decyption system makes it very difficult to analyse the virus using DEBUG as this buffer area is overwritten with every DOS call.

One file is infected whenever a DIR command is used. This is done by trapping DOS function 36h (Get Drive Allocation Information) which is used when calculating free disk space. You expect a delay at this point, when doing a DIR, so don't notice the time taken to infect. When the file is infected the seconds field of the file date/time is set to 36.

Variants

1099.

Many Fingers

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

1,322 to 1,337 bytes.

 Copyright © Dr Solomon's Software

Description

The virus contains the text **CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR.** This is displayed 1,500 keystrokes after infection, and the system is halted. This only happens on or after 11/11/1990.

Manzon

Type

Memory resident file virus.

Affects

COM and EXE files (but COM files longer than 62,000 bytes are not infected).

File Growth

Variable; usually in the range 1,430 to 1,488 bytes.

Description

The virus is double-encrypted. It uses function call AX=DCBA/INT_21 to determine whether it is already resident in memory; the correct answer is DX=DCBA.

Manzon uses normal DOS calls (AH=48) to install itself in memory; and occupies 1,728 memory bytes. It intercepts open (3D00), execute (4B00) and delete (3E) instructions. The virus does not intercept INT_24 and does not supress the 'Write protect error . . .' when trying to infect a write-protected floppy disk.

Manzon uses instructions specific to the 80286 processor and cannot work on a PC/XT.

The virus recognises some filenames and avoids infecting files containing the following strings:

F-*.*, K-*.*, SC*.*, TB*.*, TO*.*, FV*.*, FI*.* and VI*.*.

It contains a string **MANZON (c) Sgg1F5PZ^V**.

Variants

1404, 1414.

Copyright © Dr Solomon's Software

Mardi

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

On floppy disks the virus uses sectors on track 41. The infected boot sectors contain **`Sudah ada vaksin`**, which is sometimes displayed. The virus uses 7Kb of memory.

There are similarities with *Den Zuk*.

Markt (VCL.Markt, Mediamarkt, VCL-Werbe, VCL-3.DI)

Type

File virus.

Affects

COM files only.

File Growth

-

Description

This virus is encrypted, but text close to the end of the file is not:

`"MediaMarkt Werbe Virus '94 (c) MediaMarkt Germany The Wizard"`

On the 9th of September the virus erases the partition sector of the first hard disk and overwrites all available logical disks with random memory contents.

The virus shows a picture on a screen with a big banner at the top, reading **`"MediaMarkt"`** (white letters on a red background), a skull with blinking text **`"-=> SuXX <=-"`** on the forehead and red eyes. The message at the bottom of the screen reads:

`"Ups, all Disk's from C: to Z: Trashed! Sorry about that!"`

 Copyright © Dr Solomon's Software

"to ALL Military Inventors its Time to give us the Tachyonator!"

Variants

1533, 1548, 1551.

MG

Type

Memory resident file virus.

Affects

COM files on execution. A couple of other DOS interrupt function operations will also trigger infection.

File Growth

500 bytes.

Description

This stealth boot virus infects hard disks when booted from an infected floppy disk. disks are infected on read and write access (for example, the DIR or COPY commands).

Variants

MG1, MG2 and **MG3. MG3** does not infect files of greater than 64,768 bytes.

MGTU

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

273 bytes.

Description

There is a message in Cyrillic in the virus. It has no payload.

Copyright © Dr Solomon's Software

Michelangelo

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus infects the partition sector of the hard disk when booted from an infected floppy disk. The virus then infects any floppy disk accessed when the virus is memory resident.

Floppy disks:

360Kb: the original boot sector is copied to cylinder 0, head 1, sector 3.

Others: the original boot sector is copied to cylinder 0, head 1, sector 14 which is the last directory sector of 1.2Mb floppy disks, and the last but one of 1.44Mb floppy disks. There is no such sector on 720Kb floppy disks.

Hard disks: the original partition sector is moved to cylinder 0, head 0, sector 7 and the virus is written.

Every March 6th (Michelangelo's birthday), if the PC is an AT or PS/2, the trojan is triggered, overwriting the hard disk with nulls. On hard disks it assumes a geometry of 256 cylinders, 4 heads, 17 sectors per track.

This virus is closely related to ***Stoned***.

Microbe

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

 Copyright © Dr Solomon's Software

File Growth

-

Description

The virus contains the text **`This MICROBE is dedicated to 'Microchips Inc' Cebu City Phil. In appreciation for the quality training it provided us. 02/19/88 MICROMAGIC`**

The virus stores part of itself on cylinder 39, head 1, sectors 2 to 9. This overwrites data on that part of the disk. A counter is incremented each time this happens, and when the count reaches 164 the display is triggered. The screen is cleared and the above message is displayed. Then the PC boots normally.

The virus uses stealth; so any attempt to read the infected boot sector is re-directed to the original, clean boot sector.

Fake bad sectors are created, on the assumption that the disk is a 360Kb floppy disk.

Migram

Type

Memory resident file virus.

Affects

EXE files on execution or opening.

File Growth

1,219 to 1,221 bytes. Only files between 1,221 bytes and 64 Kb are infected.

Description

The virus contains the text **`MIGRAM VIRUS 1.0 (C) 1991 IVL.`**

If a COM file is run, the first ZIP file in the directory is deleted. If an EXE file is run on a Saturday, tracks 0 to 5 on physical device 2 are formatted, and the above message is displayed. However, physical device 2 is the third floppy disk drive so damage is unlikely.

This virus is one of the *Swami* family.

Variants

Antichrist:

Copyright © Dr Solomon's Software

Files grow by 1,008 bytes, and the virus contains the text ***.ZIP**. Whenever a file is infected the virus tries to delete the first ZIP file in the sub-directory.

Migram-Cemetery (Cemetery):

Both COM and EXE files are infected on opening and execution, causing them to grow by 1,417 bytes. It avoids files called *ND.*, for example, COMMAND.COM. The virus contains the word **CEMETERY**, and at 4 p.m. a display is triggered. At times outside 4 p.m. to 5 p.m., if a '1' is input to the serial port the PC is re-booted.

Migram-Smack (Smack):

Both COM and EXE files are infected on opening and execution, causing them to grow by 1,835 bytes. Files conforming to *ND.* (for example, COMMAND.COM), *AN.* (many scanners have such names), *HA.*, and *HK.* are avoided. The virus contains the text **This virus was written in Italy by Cracker Jack 1991 IVRL All rights reserved, please don't crack this virus!!**. There is also an insult to a lady virus researcher. When an EXE file is run on a Friday, the question **Is today Friday? (Y/N)** is displayed. Answering **Y** or **y** produces the response **Sorry but on Friday I wish not work!!** and a quit to DOS without letting the host program run. If the answer is anything else, the response **You are untruthful!! For punishment I format your HD Fat!!.** Then it formats cylinder 0 head 0 of the third floppy disk drive, five times. This is probably meant to cause damage to the hard disk but it is mis-coded. There are a lot of NOP instructions in the code for going memory resident, perhaps to fool scanners.

Minsk-1075 (Russ-1075)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

1,075 bytes.

Description

The virus is intended to corrupt DBF files. However, it does not work due to bugs in the code.

Some of the interrupt 21h calls are coded as interrupt 21 calls (i.e. INT 15h)

 Copyright © Dr Solomon's Software

To detect self prescence in memory the virus checks if the word at memory location [0:188] is 4F56. Virus eats 1088 bytes of memory.

Mirea (Lyceum)

Type

Memory resident file virus.

Affects

COM and EXE files (the 1975 variant infects COM files only).

File Growth

See Variants.

Description

Variants **1766, 1773, 1813, 2087** and **2204** are encrypted. Variant **4157** is polymorphic.

The virus intercepts interrupts 8, 9 and 21h. It checks for itself in memory by issuing a call, AH=BB/INT_21; the correct response is AH=AA. For most variants, infected files are recognised using byte FC at the file end. Infected files also have zero seconds and +100 years in the time-stamp.

Most variants contain a message, in Cyrillic characters, which is displayed if the keyboard is not touched for a long time (about half an hour). Variant **1832** prints:

```
Welcome to Lycee of Information Technologies !
```

Variant **703** drops a 45-byte file called README.!!!.

Variants

703, 930, 958, 1086, 1766, 1773, 1788, 1800, 1813, 1888a-b, 1901, 1950, 1975, 2087, 2204, 4157.

Mirror

Type

Memory resident file virus.

Affects

EXE files on execution or opening.

Copyright © Dr Solomon's Software

File Growth

924 to 940 bytes.

Description

After ten minutes, the display is changed, left for right, producing a mirror image of what should be there.

MISiS (NIKA,SEA Zharinov, Zharinov, Sea, Soft-236)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

MISiS has been found 'in the wild' at least once.

It is quite infectious and has a trivial payload. Boot and partition sectors can be infected. The virus has a memory resident payload and infection system. It has minimum stealth capability. The virus is not encrypted. The virus displays a message.

Variants

a - d.

Mix 1 (Mixer1)

Type

Memory resident file virus.

Affects

EXE files on loading, when greater than 8,192 bytes. Read/write file attributes are preserved. The memory resident part of the virus is in high memory and uses 2,048 bytes. The DOS **`Write protect error writing drive X: Abort, Retry,`**

 Copyright © Dr Solomon's Software

Ignore? message is displayed if the virus tries to infect a write-protected floppy disk.

File Growth

1,618 bytes.

Description

The most obvious effect is the garbling of serial and parallel port information, affecting modems, printers, mice, and so on. Numbers are unaffected, and the following table is used to translate characters:

abcdefghijklmnopqrstuvwxyz

ebsdapghejklmnufqrctovwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BECDAPGHYJKLMNUFQRSTOVWXIZ

For example, **Bad command or file name** becomes **Eed summend ur pela nema**.

A counter increments every time a file is infected after the virus goes memory resident, and is written to every infected file. If the count is greater than 5, 60 minutes later a bouncing ball is displayed (lower case o) which bounces off the sides of the screen. It is not deflected by letters (unlike *Italian*) but replaces letters over which it passes. After 50 minutes the keyboard handler is replaced with a routine which always turns off Caps Lock and turns on Num Lock. If the PC is then re-booted the bouncing ball is displayed.

This virus is modeled on *Icelandic*.

Variants

Mix1-b:

The files grow by slightly greater than 1,618 bytes.

Mix 2:

This infects COM and EXE files, which grow by 2,280 bytes. The last four bytes of infected files are **MIX2**, and the virus contains the strings **Strike the pauseVogue, you got to Let your body move with the music** and **I can leave you, say goodbye, i can love u if i try.....Left to my own devices i probely could**. This is encrypted and not displayed. The first string is from a Madonna album, and the second is from a Pet Shop Boys album.

Copyright © Dr Solomon's Software

The garbling effects are similar to **Mix1**. When Ctrl Alt Del is pressed, all characters on the screen are incremented or else noted.

Forty-eight minutes after going memory resident the screen trick is triggered.

Mongol (Mongolian, Mongolian Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus occupies four sectors. On an infected floppy disk, the main body of the virus is stored on the last track. On a hard disk drive, it is stored on track 0.

On the 30th of May, *Mongol* overwrites some tracks of the hard disk drive with EB FE bytes and prints the following message (which is encrypted in the virus body):

```
Mongolian Virus VERSION 1.00
Mongolian Brain Co, Ltd 1992
Today is birthday of my baby!!!
```

Month 4-6 (Agiplan)

Type

Memory resident file virus.

Affects

COM files on execution, except COMMAND.COM. Only files of less than 56Kb are infected.

File Growth

1,536 bytes.

 Copyright © Dr Solomon's Software

Description

If a file is run four months after being infected, some disk-writes are corrupted.

If a file is run after six months, the first five cylinders, all heads and sectors 1 to 9 on drives A to D inclusive are trashed.

Variants

a, b.

Monxla

Type

File virus.

Affects

A COM file in the same sub-directory, or one referred to in the PATH, on execution of an infected file. Only files between 3,840 and 64,000 bytes are infected.

File Growth

939 bytes.

Description

The text `(C) Monxla` can be found at the end of infected files.

On the 13th of any month there is a 40% chance that instead of infecting a file, the virus will patch the start with a HALT command, which stops the PC when the program is run. There is a 30% chance that it will patch it with an interrupt 19h, which on some PCs causes a re-boot and on others hangs the system.

This virus is closely related to *Vienna*.

Mosquito

Type

Memory resident file virus.

Affects

EXE files on execution.

File Growth

1,025 to 1,040 bytes.

Copyright © Dr Solomon's Software

Description

The virus contains the encrypted text **`WorZ a stopHello this is the core Rev 3 26/4/91 P 0.98c P.0.98 Rev 4 24IX89 bye bye.`** The word **`Mosquito`** is unencrypted.

On the 25th and 26th, if an infected program is run, the virus generates a critical error and the DOS message **`General failure reading drive x`** is displayed.

Variants

FaxFree.

Mule

Type

Memory resident file virus.

Affects

COM and EXE files on execution. EXE files are repeatedly infected.

File Growth

COM: 4,117 bytes.
EXE: 4,112 to 4,127 bytes.

Description

The virus contains **`Mule .`** near the beginning.

On Friday 13th, the first infected program run displays the message **`My name is Mule. It's a good time.`** and hangs the PC.

This virus is from the *Jerusalem* family.

Murphy (Murphy-1, Murphy-2, 10AM)

Type

Memory resident file virus.

Affects

COM and EXE files on execution and copying, except those smaller than the virus itself and those set to read-only. COMMAND.COM is infected immediately, so control is taken as soon as the PC is booted. Date/time are preserved.

 Copyright © Dr Solomon's Software

File Growth

Murphy-1: 1,277 bytes.
Murphy-2: 1,521 bytes.

Description

Disk error messages are disabled, but because of bugs in the code the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message may be displayed several times if the virus tries to infect a write-protected disk.

Both variants trigger when the system clock reads any time between about 10 a.m. and 11 a.m.

Variant 1: Causes the speaker to whistle at a high frequency and crackle when keys are pressed or a program run. The crackle stops when the time is changed to any time after 11 a.m., but the whistle continues.

Variant 2: Causes a dot (ASCII 07, the small diamond shape) to bounce around the screen, off the edges of the screen and any displayed characters. It does not usually corrupt text, but occasionally leaves a trail of dots on the screen and moves a few existing characters when the screen scrolls. The dot continues after the time changes.

Neither variant deliberately damages data.

Variants

Murphy-1:

As well as the above effects, this contains the message **`Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofi, USM Laboratory.`**

Murphy-2:

As well as the above effects, this contains the message **`It's me - Murphy. Copywrite (c)1990 by Lubo & Ian, Sofi, USM Laboratory.`**

Murphy-3:

As *Murphy-1*, but files grow by 1,284 bytes.

Murphy-4:

As *Murphy-2*, but files grow by 1,480 bytes.

Copyright © Dr Solomon's Software

Musicbug

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Floppy disks: Show 4Kb in lost clusters, used to store the virus code.

Hard disks: The partition sector looks normal, but at the place where the virus begins is the text **`MusicBug v1.06. Macrosoft Corp.`**. and near the end is **`-- Made in Taiwan --`**.

When the virus is in memory it uses stealth techniques to conceal itself.

The virus plays a random tune.

Nado

Type

Memory resident file virus

Affects

See description.

File Growth

-

Description

Nado is a small memory resident parasitic file virus. Variant **584** infects only EXE files. **601** infects both COM & EXE files, others infect only COM files. The virus is encrypted (apart from the *584* variant).

Variants

584, **602**,**759**, **838** and **841**.

All variants are semi-stealthing, and contain the following strings:

 Copyright © Dr Solomon's Software

584 - **"(RedViper (c) made by TorNado in Denmark '95)"**

602,759 - none

838,841 - **"(Yitzhak-Rabin 1.00 (c) made by Tornado in Denmark '96)", "anti-vir.dat"**

Nado virus corrupts the files it infects so that only part of them runs. Corrupted files cannot be repaired properly and should be replaced with good copies.

All viruses (except **584**) have damaging payloads. Variants **602**, **838** and **841** intercept keyboard interrupt (09h) and write garbage to the disk whenever the Delete key is pressed. They then hang the PC. Variant **759** does the same when DOS function SetDefaultDisk (AH=OE) is called and the current minute is 55.

Natas

Type

Multipartite virus.

Affects

COM and EXE files on execution or closing (for example, when copying a file, both source and destination are infected). COM files of greater than 60,692 bytes or less that 1,000 bytes, and EXE files of greater than 938,040 bytes are not infected. The virus also infects the partition sector and the boot sector of floppy disks.

The partition sector of the hard disk is infected when an infected program is executed, or when the PC is booted from an infected floppy disk.

Floppy disks are infected on read access (for example, within the DIR or COPY commands).

File Growth

4,744 bytes.

Description

When an infected program is run, or when the PC is booted from an infected floppy disk, *Natas* goes memory resident, infecting the partition sector. The virus does not re-locate the original partition sector. The virus patches the partition executable code, changing 41 bytes, but leaving the partition table unchanged. Additional virus code is stored on nine sectors at the end of the first track, but excluding the last sector of the first track.

Copyright © Dr Solomon's Software

Natas infects the boot sector of floppy disks which are accessed in an infected PC. The virus does not re-locate the original boot sector. The virus patches the boot sector, changing 41 bytes. Additional virus code is stored on nine sectors at the end of the disk and the BIOS Parameter Block (BPB) is patched to ensure that these sectors are not overwritten by data.

Files infected by *Natas* are variably encrypted and polymorphic.

Natas uses stealth to conceal itself when memory resident. If the partition sector is examined when the virus is memory resident, the original partition sector is displayed. The virus does NOT conceal the additional virus code at the end of the first track. Unlike most full stealth viruses, *Natas* can survive backups (BACKUP, PCBACKUP), archiving (ARJ, LHARC, PKZIP), and transfers of infected files via modem (ZMODEM, XMODEM, and so on). Also, it does not trigger CHKDSK file system error reports. *Natas* also uses stealth to conceal the increase in file size.

When the PC is booted from an infected hard disk, there is an approximate 1-in-512 chance that the virus will trigger, formatting all hard disks in the system, and destroying all data on them. The virus can also trigger when being traced with a debugger.

It has encrypted strings **`Natas,`** **`BACK`** and **`MODEM`**.

The author of this virus, who also wrote *SatanBug*, is known to the authorities.

IMPORTANT: Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS disk, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will NOT be detected by a scanner which fails to detect the virus in memory and which scans the files with the virus active in memory. For this reason, Dr Solomon's strongly recommend that the Anti-Virus Toolkit programs are run from the original write-protected floppy disk until the virus has been removed. FindVirus will find *Natas* in memory as a safety measure.

Necropolis

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

 Copyright © Dr Solomon's Software

File Growth

1,963 bytes. One cluster is added to the FAT chain of files without changing the directory entry. This is used to store the virus code. When the virus is in memory, files look normal to a DOS read.

Description

Necropolis uses stealth to conceal the increase in file size. This virus makes extensive use of tunneling, going under interrupts 21h and 13h when it writes to disk, ensuring that generic monitoring programs cannot detect the writes.

Most DOS functions are trapped and re-defined to achieve the stealth effect.

Variants

Necrophylia-b:

Forty bytes have been patched to put in the message **`(C) by Cracker Jack 1991 - IVRL NeCrOpHyLiA.`** The variant does not work properly.

Necros.1164

Type

Memory resident file virus.

Affects

COM files by appending the body of the virus to the original file. EXE files using the companion technique.

File Growth

-

Description

The virus is polymorphic. It has two internal strings:

```
Virus V2.0 [FrIEND]i
```

and

```
Virus V2.0 (c) 1991 Necros The Hacker
Written on 29, 30 June in Tralee, Co. Kerry, Ireland
Happy Birthday, Necros!
```

The first string is visible in the memory. The second string is encrypted. On the 21st of November, the virus causes the PC to beep and the second string is printed.

Copyright © Dr Solomon's Software

Neuroquila (Havoc, Neuro.Havoc, Wedding)

Type

Multipartite virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk, or if an infected EXE file is run.

File Growth

-

Description

Neuroquila.mp is a memory resident, multipartite virus. Where possible, it loads into the Upper Memory Blocks (UMB) provided by EMM386. The virus uses stealth to conceal changes it makes to infected partition sectors and floppy disk boot sectors. On floppy disks, the virus formats an additional track and uses this to store the main body of the virus code. This virus is able to modify some TSR anti-virus programs in memory (for example, TBDRIVER, TBDISK, VSAFE).

Neuroquila encrypts the partition sector. As a result, the hard disk becomes inaccessible if the PC is booted from a DOS system disk. If FDISK /MBR is used to remove this virus, the hard disk will become inaccessible (it is inadvisable to use FDISK /MBR to remove any virus).

Neuroquila is, in some respects similar to the *Tequila.mp* virus; hence its name. It was written by the virus writer calling himself Neurobasher (author of *Tremor* and *Nightfall*). *Neuroquila.mp* [.a] contains a string (which is displayed a couple of months after the PC becomes infected):

```
<HAVOC> by Neurobasher'93/Germany
- GRIPPED BY FEAR - UNTIL DEATH US DO PART!
```

Nightfall (N8Fall, Neurobasher.N8Fall)

Type

Memory resident file virus.

Affects

COM and EXE files.

 Copyright © Dr Solomon's Software

File Growth

See Variants.

Description

Nightfall is a memory resident polymorphic virus. Where possible, it loads into the High Memory Area (HMA) provided by HIMEM.SYS or the Upper Memory Blocks (UMB) provided by EMM386; but the short memory dispatcher is always located in low memory, at 0:5E0.

It uses stealth to conceal itself when memory resident and is also a fast infector (infecting files not only on execution, but also when copied or opened).

Nightfall avoids infecting files containing the strings AV, PL, CH and MI. In addition, it disables VSAFE by patching it in memory.

The virus requires at least a 386 processor; some specific commands are used by the polymorphic engine in the virus decryptor.

Nightfall sometimes drops the *Nightfall.cmp.527* resident companion virus in EXE files. This companion deletes itself after it runs. It avoids infecting files on floppy disks (probably because it is slow).

Nightfall was written by German virus writer calling himself Neurobasher (author of *Tremor* and *Neuroquila*). The virus contains the following text:

```
   Any means necessary for survival

      _ N8Fall/2XS by NeuroBasher _

By the perception of illusion we experience

                  reality

Art & Strategy by Neurobasher 1994 - Germany

I don't think that the real violence has even

                started yet
```

Variants

4518a-b, 4527, 5767.

Nina (Happy New Year 1600, V1600)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution. COMMAND.COM is avoided.

File Growth

1,600 bytes. EXE files vary slightly from this value.

Description

The virus contains the text **`Dear Nina, you make me write this virus; Happy new year!.`**

Whenever information is written to a file, the boot sector is read, one word is changed at offset 3 (the OEM label) and then written back.

This virus appears to be a re-write of *Jerusalem*.

Nina 2 (Nina-256)

Type

Memory resident file virus.

Affects

COM files on execution, except those between 500 and 65,200 bytes long and those set to read-only.

File Growth

256 bytes.

Description

The virus contains the text **`Nina,`** and has no payload.

It is completely different from *Nina*.

NJH (LBC, Korea Boot, NJH-LBC, NJH2LBC)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk. The viruses uses 2Kb from the top of memory.

Copyright © Dr Solomon's Software

File Growth

-

Description

Infected boot sectors contain the text **`virse program messge Njh to Lbc.`**

The virus replaces the boot sector of floppy disks with its own code and moves the original boot sector further up the disk. On a hard disk it re-locates the partition sector.

No intentional damage is done, but because the place where the original boot sector is stored does not vary with the type of disk, problems may occur on disks of capacity greater than 360Kb. There is a test in the virus to avoid infecting hard disks, but it does not work.

Floppy disks are inoculated against *Brain* and *Ping Pong*.

Variants

NJH2LBC.a.

No Bock

Type

File virus.

Affects

A random number of COM files on execution of infected files, provided they are between 2,000 and 64,000 bytes long.

File Growth

440 bytes.

Description

If a file is run nine months after it is infected, the message **`No Bock today Error, System halted!`** is displayed and the system hangs.

No_Frills

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files.

File Growth

See Variants

Description

No_Frills infects COM and EXE files when they are executed, opened or copied. The 1358 variant infects COM files only.

The virus intercepts INT_21 functions 3D (Open), 43 (Get Attribute), 4B (Execute), 6C (Extended Open; not used by .1358). It checks for itself in memory by issuing a call, AX=5432/INT_21h; the correct response is AX=1005 (.813, .815, .843), AX=1006, (.950), AX=1007 (.835, .840), AX=1301 (.1358).

No_Frills does not infect files starting with SC (for example, SCAN.EXE).

Files are misinfected quite frequently by the No_Frills viruses.

This family of viruses is related to ***X-Fungus***.

The following strings are found in these viruses:

```
813:  +-No Frills by Harry McBungus-+

815a: +-No Frills 1.01 by Harry McBungus-+

815b: +-No Frills by Harry McBungus-+

835:  +-NF3.0-H.McB-[PuKE]-+

840:  no strings

843:  +-No Frills 2.0 by Harry McBungus-+

950:  +-K-Lame Kreation by Harry McBungus-+

1358: Kcat 3.01 ñ 5%  -  By Sir Twist & Thunderbird,
      with Many Thankz to Harry McBungus whose coded
      we politely nicked.
```

Variants

813, 815ab, 835, 840, 843, 950, 1358.

Copyright © Dr Solomon's Software

No_Frills.Dudley.1153

Type

Memory resident file virus.

Affects

COM and EXE files (variant 1358 infects COM files only).

File Growth

1153 bytes.

Description

This is a memory resident polymorphic virus. It is a fast infector, infecting files when they are executed, opened, copied or renamed.

The virus intercepts INT_21 functions 3D (Open), 4B00 (Execute), 56 (Rename) and 6C (Extended Open). It checks for itself in memory by issuing a call, AX=5454/ INT_21h; the correct response is AX=0.

All infected files start with the bytes 71 00 - this is an infection marker for COM files. EXE files are marked by EP (50 45) in the checksum field of the EXE header.

This virus does not infect files starting with SC (for example, SCAN.EXE).

It contains the string:

```
"<[Oi, Dudley!][PuKE]>"
```

Noint (Bloomington)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Noint is one of the many variants of *Stoned* virus. *Noint* infects the boot sector of floppy disks and the partition sector of hard disks. The partition sector becomes

Copyright © Dr Solomon's Software

infected when the PC is booted from an infected floppy disk (even if the floppy disk is not bootable). The virus then goes memory resident, infecting floppy disks which are accessed (even if floppy disks are just being read). The virus uses stealth to conceal itself when memory resident. The original partition sector is re-located to cylinder 0, head 0, sector 7. On floppy disks, the original boot sector is re-located to one of the root directory sectors.

Nomenklatura (Nomen)

Type

Memory resident file virus.

Affects

COM and EXE files on execution, if they are greater than 1,024 bytes and COM files less than 64,000 bytes.

File Growth

1,024 bytes.

Description

The virus contains the text **`Nomenklatura`**. The FAT is gradually corrupted by swapping words in the memory copy of the FAT where there are long FAT chains (large files). DOS then writes the memory copy of the FAT to disk as normal. This is done so that monitor-type programs cannot prevent the corruption.

There are a number of similarities to the *Live after Death* series, for example in the payload code.

The damage done by *Nomenklatura* is gradual and subtle, which means that it could be a long while before it is discovered, by which time the corrupted files may have been backed up many times.

Variants

Nomenklatura.a:

Nomenklatura.b:

Because of a corruption in the code, if it tries to infect an EXE file, it causes system problems such as **Divide by zero**, or the system hangs.

Copyright © Dr Solomon's Software

Noon-beep (Milous)

Type

Memory resident file virus.

Affects

COM files on execution. Files must be between 32 and 62,464 bytes long.

File Growth

1,163 bytes.

Description

At 12 noon, the speaker gives three short beeps and a long one. The virus contains a routine to remove itself from files.

Nov17 (November_17th, BigMouse)

Type

Memory resident file virus.

Affects

COM and EXE files (except the 584 variant, which infects COM files only).

File Growth

See Variants.

Description

Nov17 is not encrypted (except variants **900**, **998** and **1007**). All unencrypted host files have the marker MZ as the last two bytes of the file (except **Nov17.584**; and in the **864** variant, the marker is 11 bytes below the end of file).

The most common variants of this virus (**768a**, **800a**, **855a**) do not use a simple jump to transfer control to the virus. They push two words on to the stack (code segment value and offset of the viral code) and then do a far return, which transfers control to the beginning of the virus.

Variants **768**, **800**, **855**, **864**, **880** contain the following string, close to the end of the file:

```
SCAN.CLEAN.COMEXE
```

Copyright © Dr Solomon's Software

Encrypted variants (**900, 998** and **1007**; variant **1006** is a virus 'wannabe' (or intended virus) and does not work properly) use INT_FF to decrypt themselves; and carry a list of anti-virus programs they do not infect (the first 4 letters):

SCANCLEAVIRSF-PRCPAV

Variants

584, 690, 706a-b, 768, 800a-c, 855a-b, 864, 880, 900a-c, 998, 1006, 1007.

Variants of this virus have the following payloads (all disk-oriented payloads use INT_26 to overwrite the beginning of the current drive; the only exception is **Nov17.706**, which uses INT_13):

584 erases CMOS on Wednesdays, if the current hour is in the range 13-16.

690 erases the first 8 sectors of the current drive, on 8 July.

706 overwrites the first 11 sectors of the current drive (but not C and D drives), on the 1st of any month.

768a,c,d and **800a** erase the first 8 sectors of the current drive, between 17 and 30 November.

768b erases the first 8 sectors of the current drive, on the 8 July.

800b erases the first 8 sectors of the current drive, on 1 January.

855 erases the first 8 sectors of the current drive after 500 keypresses, between 17 and 30 November.

864 erases the first 8 sectors of the current drive, between 10 and 30 July.

880 erases the first 4 sectors of the current drive after 100 keypresses, between 17 and 31 October.

900a prints **G+A= , Press a key to go on** (if current year is greater than 1993), on 23rd of any month.

900b,c print the 900a message, but only on 23 November.

998 sometimes overwrites sectors on the current drive, in April.

1007 prints the message:

BigMouse and Anna love each other

Press any key to go on

on 23rd of November.

 Copyright © Dr Solomon's Software

Npox.963 (Nuke.Pox, Genius, Evil Genius)

Type

Memory resident, file virus.

Affects

COM and EXE files.

File Growth

963 bytes.

Description

The virus is a semi-stealth virus as it conceals the change in size of infected files. However, it does not intercept interrupt 24, so execution of a program on a write-protected floppy disk produces the DOS message **`Write-protect error writing drive X:`** if the virus tries to infect files on a write-protected floppy disk.

The virus also intercepts the keyboard vector (interrupt 09) and uses this for its payload. On the 24th of any month, when Del is pressed, the virus tries to format the hard disk drive, but this works only on very old MFM hard disks (on other types of hard disk the PC just hangs), and then causes a re-boot.

Variants

a-c.

Variant a:

This variant contains the string:

```
Evil Genius V2.0 - R.S/NuKEC:.COM
```

Variant c:

This variant contains the string:

```
(c) 1992 by Igor Ratzkopf - All rights reserved July R
```

There are also other variants of the virus belonging to the same family. These variants have the following byte-lengths: **609, 630, 900, 955, 1482, 1686, 1708, 1722, 1723, 1800,** and **1844**.

Copyright © Dr Solomon's Software

Number of the Beast (NotB, V512, 666)

Type

Memory resident file virus.

Affects

COM files on execution of certain DOS functions, for example, copying, executing, reading. Read/write attributes and date/time are preserved.

File Growth

None apparent. The virus is inserted into unused space at the end of the last cluster of the file.

Description

This virus is a stealth virus and hides itself very well. Some DOS utilities may give inappropriate error messages.

There is no payload. It appears to have been written as an exercise in using the internal workings of DOS. However, an infected file will work only if it is copied after the virus goes memory resident. If it is copied before this, this copy of the virus will not work, although the virus will still go memory resident and infect programs run subsequently.

The virus hides itself in memory so that it is invisible to most memory map programs and monitors. It also identifies files that it has already infected by changing the seconds field in the time-stamp to 62, although this is not visible using DIR.

This virus has been written by an extremely cunning author and uses many undocumented features of DOS. It is signed **666** at the end, hence the name.

Variants

There are 13 variants, all functionally identical, differing only in implementation of the code.

IMPORTANT: Because the virus hides itself, it is vitally important that all work on infected systems be done after booting from a clean, write-protected DOS disk, and all software run must be known to be clean. If an infected program is run, all executables accessed subsequently will be infected and this will NOT be detected by a scanner which fails to detect the virus in memory and which scans the files with the virus active in memory. For this reason, Dr Solomon's strongly recommend that the Anti-Virus Toolkit programs are run from the original write-protected floppy disk until the virus has been removed. FindVirus will find *Number of the Beast* in memory as a safety measure.

 Copyright © Dr Solomon's Software

Number One (Burger-Pascal)

Type

Overwriting file virus.

Affects

A COM file in the same directory on execution of an infected program.

File Growth

None. The virus overwrites the first 12,032 to 13,952 bytes.

Description

The virus contains the string **`This file has been infected by Number One`**. If all files have been infected the message **`<smile>`** is displayed.

This virus was first published in the Burger book in Pascal source code.

Variants

Number 1.b:

Each infected program announces itself by displaying **`The Fie Has Been Infected by Number One.`**

NYB (B1, New York Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

If the PC is booted from an infected floppy disk, the virus transfers itself to the partition sector of the hard disk. When the PC is next re-booted the virus goes memory resident and will infect floppy disks when they are accessed in drive A.

Copyright © Dr Solomon's Software

On hard disks, the virus copies the original partition sector to cylinder 0, head 0, sector 17. On floppy disks, the original boot sector is copied to the last sector of the root directory.

When the virus is in memory, it uses stealth to conceal itself. If the partition sector or the boot sector is examined, the virus displays the original clean partition or boot sector

The virus has no payload.

Odious.569

Type

File virus.

Affects

COM files.

File Growth

569 bytes.

Description

Odious is a non-encrypted virus, infecting COM files only. It is non-resident. The virus appends its code to infected files. It always infects COMMAND.COM.

On any Monday in May, the virus causes some characters on the screen to disappear (by clearing their definition in the current font). It has no destructive payload.

The virus contains the following strings: **`The Creeper Virus V2.0`**, **`*.com`**, **`c:\chklist.*`** and **`c:\command.com`**.

Ogre (Computer Ogre, Disk Killer, Disk Ogre)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

 Copyright © Dr Solomon's Software

File Growth

-

Description

If an infected PC is left on for 48 hours and the hard disk is accessed during the next hour, the virus is triggered. The screen clears and the virus displays:

```
Disk killer - Version 1.00 by COMPUTER OGRE 04/01/1989

Warning !!

Don't turn off the power or remove the disk while Disk killer
is processing!

PROCESSING
```

The virus then encrypts the contents of the bootable partition sector.

An infected PC loses 8Kb of memory, and infected disks have 3Kb of bad sectors.

Floppy disks: the original boot sector is moved up the disk. Because the wrong group of sectors is marked as bad, *Ogre* leaves itself vulnerable to being overwritten by data placed on the disk later.

Hard disks: the boot sector is moved up the disk.

Variants

There is a variant where the message contains `Version 1.04`.

Old Yankee

Type

File virus.

Affects

EXE files on execution of an infected file.

File Growth

Two versions: 1,961 and 1,624 bytes.

Description

The virus plays Yankee Doodle when an infected program is run.

This is very different from *Yankee Doodle* which also plays Yankee Doodle.

Copyright © Dr Solomon's Software

Omega (Friday-13th-440)

Type

File virus.

Affects

COM files in every sub-directory on drive C, on execution of the infected file.

File Growth

440 bytes.

Description

When an infected program is run there is a lot of disk activity as each COM file on the hard disk is read to see if it is already infected.

On every Friday 13th the payload is triggered. This overwrites the hard disk, cylinder 0, head 0, sectors 1 to 8 of the hard disk, with garbage; it then does the same to cylinder 0, head 1, sectors 1 to 8. The first overwrite hits the partition sector, and the second will overwrite the boot sector and part of the FAT on most PCs.

This is one of several viruses called ***Friday 13th*** – see also ***Virus-B*** and ***Jerusalem***.

ON 64 (V696)

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

696 bytes after padding to a multiple of 16 bytes.

Description

After 64 infections the trojan triggers, overwriting the first four heads of cylinder 0 of the hard disk.

One-Half (Dis, Free Love, Slovak Bomber, Explosion-II)

Type

Multipartite virus.

 Copyright © Dr Solomon's Software

Affects

Fast infector. Infects COM and EXE files on execution, opening, renaming, and so on. The partition sector of the hard disk is infected when an infected program is executed.

File Growth

3,544 bytes.

Description

The virus reduces the size of DOS memory by 4Kb. When the virus is memory resident, it uses stealth to conceal itself, also concealing its own code. The virus is also polymorphic. ***One-Half*** is a 'fast infector', infecting files not only on load-and-execute but also on open, rename, etc. For this reason it is essential that scanners are able to detect the virus if it is active in memory.

The virus uses 'tunneling' (traces INT_13 to get original interrupt entry point).

The virus hooks interrupts 01, 13, 1C, 21 (functions 11, 12, 3C, 3D, 3E, 4B00, 4C, 4E, 4F, 56, 5B, 6C00) and 24. Self-recognition is INT_21 with AX=4B53 and the correct response is AX+454B. The virus recognizes SCAN, CLEAN, FINDVIRU, GUARD, VSAFE, NOD and MSAV by name and does not infect them.

The virus re-locates the original clean, partition sector further along the first track, eight sectors before the boot sector. Additional virus code is stored in several sectors following this sector, including one sector which contains the text:

```
Dis is one half
```

```
Press any key to continue.....
```

and

```
Did you leave the room ?
```
(which is never displayed).

The nastiest feature of ***One Half*** is its payload. Each time you re-boot the PC, the virus encrypts two tracks of the drive. While the virus is in memory, it decrypts these tracks 'on-the-fly', so that all the data appears normal. However, if the method used to remove the virus does not decrypt these cylinders, the data will be inaccessible. For this reason, FDISK/MBR should not be used to remove this virus.

Variants

There are three known variants identified by the file growth: 3544 bytes, 3,577 bytes, and 3570 bytes.

Copyright © Dr Solomon's Software

Ontario.1024 (SBC)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. COMMAND.COM is infected immediately. COM files must be less than 57,335 bytes.

File Growth

COM: 512 bytes.
EXE: 536 to 688 bytes.

Description

There is no payload.

Oropax (Music virus, Musician)

Type

Memory resident file virus.

Affects

The next COM file in the current sub-directory when a sub-directory is created or removed, or a file is created, opened for writing, deleted or renamed. COMMAND.COM is avoided.

File Growth

2,756 to 2,806 bytes to a multiple of 51 bytes.

Description

One in four times, five minutes after the virus goes memory resident, it plays one of three tunes every seven minutes. These are:

The Stars and Stripes For Ever

Mozart's Symphony No. 40

The Blue Danube

Oropax is a brand of German earplugs.

Copyright © Dr Solomon's Software

Paris (TCC)

Type

File virus.

Affects

An uninfected COM or EXE file on execution of an infected file.

File Growth

4,909 to 4,934 bytes. COM files must be less than 58,368 bytes long to be infected.

Description

The virus fails to work correctly on hard disks with capacities other than 10Mb or 20Mb.

Parity

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

441 bytes.

Description

When an infected file is run, there is a 3% probability that the message **`PARITY CHECK 2 2000 (S)`** will be displayed and that the PC will hang.

Parity.b

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

Copyright © Dr Solomon's Software

File Growth

-

Description

If the PC is booted from an infected floppy disk, the virus infects the partition sector of the hard disk. **NOTE:** If the PC is switched off when the **`Non-system disk or disk error, replace and press any key when ready message`** is displayed, the virus does NOT infect the hard disk (this is unusual for boot sector viruses; and it is always wise to assume that the hard disk will be infected, irrespective of whether the PC is switched off at this point). The virus infects any floppy disk which is accessed with the virus memory resident.

On hard disks, the virus copies the original partition sector to cylinder 0, head 0, sector 14. On floppy disks, the original boot sector is copied to one of the root directory sectors.

When the virus is memory resident, it uses stealth to conceal itself on the hard disk. If the partition sector is examined, the virus displays the original, clean partition sector. However, it does not stealth 0, 0, 14 and the original partition sector can be seen.

If the virus attempts to infect a write-protected floppy disk, it will perform an infinite loop when trying to infect it, causing the PC to hang. If no floppy disks are infected for approximately one hour, the virus triggers; on the next keystroke it displays **`PARITY CHECK`** and hangs the PC.

This virus survives a warm re-boot. For this reason, it is essential to use a power-off re-boot before attempting to remove this virus.

PcVrsDs

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

1,904 bytes. EXE files are rounded to a multiple of 16 bytes. The virus uses stealth to conceal itself when memory resident.

 Copyright © Dr Solomon's Software

Description

Encrypted inside the virus is the text **`PcVrsDs Version 1.00 Copyright (C) VirOP 1990`**.

If the year is set to 1990 the virus infects 16 files and then deletes any file run or opened. In 1991 or after, this happens after six infections.

On Monday (but not in 1990, or on the 23rd), the virus waits for 255 keystrokes, then every 14th keystroke is altered to produce the next higher ASCII character.

On the 23rd (but not a Monday) programs infected will not run later on, unless the virus is already in memory when you try to run them.

Ten days after any Friday 13th the payload is triggered. This does a low-level format of the hard disk, cylinders 0 to 31, head 0. Then the above message is displayed.

There is a resemblance to *Jerusalem*, but the differences are substantial.

Perfume

Type

Memory resident file virus.

Affects

COM files on execution. Read/write file attributes are preserved.

File Growth

765 bytes.

Description

When infecting a file, four bytes are added at the end. The first two of these are the self-recognition code VI, and the second two are a counter initialized to 0. Every time the file is run the counter is incremented, and when it reaches 80 a message is displayed before the program is run. The first is **`Bitte gebe den G-virus Code ein`**, and the second is **`Tut mir Leid (Sorry)`**.

If **`4711`** is typed in response to the message, the program continues. Typing anything else produces a second message and the program terminates with a return code of 1, which is an error level usually produced by abnormal termination (crashing).

In one sample the message is replaced by nulls. 4711 is a famous perfume.

Copyright © Dr Solomon's Software

Variants

Perfume-731:

COM files grow by 731 bytes. The messages are intact.

Other variants are: **Perfume.blank, Perfume.message**, and **Perfume.Slash**.

Peter (Peter II)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus has a memory resident infection system. It has advanced stealth capability. Some messages in the virus are encrypted. The main message is:

```
256 Kb CACHE MEMORY
33Mhz CPU Clock
Good Morning, EVERYBODY, I am PETER II

Do not turn off the power, or you will lost all of the data in
Hardisk!!!

WAIT for 1 MINUTES, please...

Ok.If you give the right answer to the following questions, I
will save your HD:

A. Who has sung the song called "I'll be there" ?

   1. Mariah Carey   2. The Escape Club
   3. The Jackson five  4.  All (1-4) : 4

B. What is Phil Collins ?

   1. A singer   2. A drummer
   3. A producer  4.  Above all (1-4) : 4
```

 Copyright © Dr Solomon's Software

```
C. Who has the MOST TOP 10 singles in 1980's ?

   1. Michael Jackson   2. Phil Collins (featuring Genesis)
   3. Madonna  4.  Whitney Houston (1-4) : 2

CONGRATULATIONS  ! ! !  YOU successfully pass the quiz!
AND NOW RECOVERING YOUR HARDISK ......
```

PH33R.1332 (WordMacro.Nuclear.1332, Kamikaze)

Type

Memory resident file virus.

Affects

COM and EXE files (but no COM files shorter than 1,024 bytes and longer than 60,000 bytes).

File Growth

-

Description

This virus also infects NE executable files (the format of Microsoft Windows 16-bit EXE files).

Infected EXE files are marked with the word AFAF at offset 12h (the checksum field, which is ignored by DOS). COM files start with a jump, after which is AF, used by the virus for self-recognition.

All infected NE executables have the time-stamp 3-10-92, 3:10:00a (which is exactly how all Microsoft Windows 3.10 files are set).

This virus was written by an Australian group of virus writers (VLAD). The macro virus *WM.Nuclear.a* contains a payload to drop this virus; but this fails because of numerous bugs.

Phoenix phoenix (Live after Death 4)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM files on execution. Files of some sizes are avoided so approximately 1-in-8 files will be unaffected.

File Growth

1,704 bytes. COMMAND.COM is infected without growth.

Description

The virus contains the encrypted text **PHOENIX**. The encryption and decryptor/loader are variable.

The FAT is gradually corrupted by occasional swapping of two entries in the sector buffer. This means that anything monitoring disk-writes fails to see the corruption as it happens in memory before DOS does the write. At the interrupt 13h level, some reads are converted to writes and some EXE files are trojanized.

Phx (Pux, PUX, Tracker)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

Description

Phx is a memory resident appending virus, infecting COM and EXE upon execution. The most common variant is **PHX 965**. It has a complex payload which has almost no effect. Sometimes the virus changes one bit in memory but it happens rarely. Variant **PHX 965** contains a short string **'PHX'**.

This virus does not work on XT computers as it uses 80286 instructions. The **PHX.1289** variant only works under DOS version 3.

Variants

PHX.1289, PHX.1295, PHX.823, PHX.965, PHX.1015, PHX.1360.

 Copyright © Dr Solomon's Software

Pindonga.3580

Type

Memory resident file virus.

Affects

COM and EXE files. Only COM files starting with a JMP (E9 instruction) are infected.

File Growth

-

Description

The virus is polymorphic. It has two internal strings:

```
PINDONGA Virus V4.3 (Hecho en ARGENTINA)
```

and

```
PINDONGA virus (Programado por OTTO en ARGENTINA 16977
```

The first string is encrypted in the body of the virus. The second string is not encrypted.

On 25th February, 21st March, 27th August, and 16th September, the virus is triggered and erases the data on the hard disk. To get the date the virus uses direct access to the CMOS/clock ports (70h, 71h).

When the virus execution is finished, the virus does not restore the initial jump of the host COM file, it simply jumps to the location where the original JMP used to point.

Ping Pong (Italian; Ping Pong-B; Bouncing Ball; Mistake; Bouncing dot; Vera Cruz; Turin)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk. 8086 and 8088 (XT) machines are affected.

File Growth

-

Copyright © Dr Solomon's Software

Description

Once every 30 minutes, if the disk is being accessed, a bouncing dot is triggered on the screen. Infected disks have one cluster (1Kb or 512 bytes) of bad sectors and hard disks lose one cluster (usually 2Kb).

This virus replaces the boot sector of a disk with its own code and moves the original boot sector further up the disk. The virus has no ill effects other than slowing down the floppy disk drive and making 2Kb of memory unavailable to DOS.

Variants

Big Italian:

This generates a diamond shape instead of a dot and will infect 80286 and 80386 machines.

Mistake (Typo; Typoboot):

This exchanges characters while they are being output to the printer, using the following substitution table:

18CKGJMNOU36VW27ckgjmnou49vw

1 is substituted for 8 and vice-versa, C for K, and so on. It also does a substitution on some of the high-order bytes:

80h 92h 9Ah 88h 97h 8Bh 85h 8Fh

This is more meaningful when the Hebrew character set is used.

NOTE: The ***Fumble*** virus, which is quite different, is also sometimes called ***Typo***.

Pinworm (Virogen.Pinworm)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

Pinworm is a memory resident polymorphic virus infecting COM and EXE files which are executed.

 Copyright © Dr Solomon's Software

The virus removes the files CHKLIST.MS and CHKLIST.CPS (MSAV and CPAV integrity database files, respectively) and is also able to corrupt executable files of anti-virus products named *AV.*, *.OT.*, *SCAN.* (NAV, F-PROT, SCAN).

The payload of the most common ***Pinworm*** virus (the 2150 variant) activates on the 1st of any month. The virus creates a sub-directory called PÏïWérM.ûg! containing a number of files. These files have spaces in the file names and form a short text:

```
I hope y
ou have
enjoyed
your inf
estation
by the
mighty P
inworm p
arasite
Fuck you
all!
úúúúúúúú (this is ASCII 250)
-ûirogen
```

The virus also contains a string:

```
v1.00 - Coded by ûirogen in April 1994
CHKLIST.MS CHKLIST.CPS
```

Variants

1800, 2400, 2150, 2171, 2371, 2566, 2585, 2780.

Pirates Hat.2360

Type

Memory resident file virus.

Affects

EXE files on execution.

Copyright © Dr Solomon's Software

File Growth

-

Description

This virus is highly polymorphic. It uses a very complicated mechanism to build a decryptor for itself.

The virus contains an internal string:

```
[For pirates... (C)1993-94 nessuno] sono solo stronzate.
```

It is visible only in memory, as all infected EXE files are encrypted.

Some infected files (less than 1-in-200) are damaged during the infection process and will hang the PC if executed. The virus frequently sets negative values for the CS register in the EXE file header, so if the PC has free RAM space of 620Kb or greater, the virus might hang the PC.

Piter

Type

Memory resident file virus.

Affects

COM files on execution, provided they are between 2,000 and 64,000 bytes long.

File Growth

529 bytes.

Description

The first time an infected program is run, the virus goes memory resident and the program does not run.

Pixel

Type

File virus.

Affects

COM files on execution, including COMMAND.COM.

Copyright © Dr Solomon's Software

File Growth

Varies according to the version (see Variants).
Date/time and read/write attributes are preserved in some files and not others.

Description

The virus has a counter which keeps track of the generation number. After the 5th generation there is 50% probability of getting the message **`Program sick error:Call doctor or buy PIXEL for cure description`** when an infected file is run.

This virus was allegedly published in a Greek PC magazine in BASIC. When this program is run it creates a COM file, which is the virus. It reached Bulgaria in this form and was then worked on by various programmers to create new versions.

Variants

All of these variants are almost functionally equivalent to the original, but attempts seem to have been made to reduce the byte-count of the virus.

Pixel-905:

As **Pixel-897**, but only on or after the 3rd generation.

Pixel-899:

As **Pixel-897**.

Pixel-899b:

Formats the third floppy disk drive, if present.

Pixel-897:

Looks for dates on or after April 1st, when there is a 50% chance of the payload triggering. This displays the message and formats drive A, cylinder 0, head 0.

Pixel-892:

After the third generation, as **Pixel-905**, but the message is obscene.

Pixel-877:

On the ninth generation the message **`Sector not found error fucking defoult drive! Please buy me a new disk drive!`** is displayed.

Pixel-854:

The message is in Cyrillic.

Copyright © Dr Solomon's Software

Pixel-850:

As in the previous description.

Pixel-847:

This is the original version. The self-recognition code is **VI** in bytes 3 and 4 of the file. Read-only files are not infected.

Pixel-837:

The message is **`I love you so much!!! -- Francis`**.

Pixel-779:

As in the above description.

Pixel-345:

This corrects the major bug in **847**, which meant that what was copied was far too long. The self-recognition code is at bytes 2 and 3.

Pixel-299:

Date/time are preserved, and it uses the Disk Transfer Area instead of defining a local one, which reduces the byte-count.

Pixel-295:

As in the above description.

Pixel-283:

Triggers at the 16th generation. The message is **`What a stupid you are !!!!!!!!.`**

Pixel-277 (V-277):

The message is absent and replaced by a beep which never happens because of a bug in the code which tests for a 50% chance to do it. The self-recognition code is **UM** in bytes 2 and 3.

Pixel-275:

Triggers at the second generation. The message is **`Fucking hell:You wet pussy.`**

Pixel-Year-6545:

Files grow by 936 bytes. On April 1st year 6545 and thereafter the virus displays a message and formats cylinder 0 of a floppy disk in drive A. The message starts with

 Copyright © Dr Solomon's Software

some obscenities, then continues **HaHaHa... What a Good Friday!!.** The year is because of a bug which confuses hex and ASCII.

Nocargar:

This is **Pixel-847** with the message changed to **En Tu PC hay un virus RV1, yesta Es su quinta generacion**.

Luz (Advert):

Files grow by 847 bytes and the date/time is not preserved. The message is changed to **Hello, John Mcafee,please uprade me.Bests regards,Jean Luz**.

There are further versions which increase file sizes by 740 and 257 bytes.

PKZ300 trojan

Type

Trojan

Affects

-

File Growth

-

Description

An executable file inside a self-extracting ZIP archive named PKZ300B.EXE (the size is 178,981 bytes).

The self-extracting archive contains the following files:

PKZINST.EXE	5,328 bytes (uncompressed length)
WHATSNEW.300	2,417 bytes
COMPRESS.000	124,005 bytes
COMPRESS.001	116,260 bytes
FILE.ID.DIZ	101 bytes

The first file - PKZINST.EXE is a HLL program (apparently written in Pascal), which is a trojan. When started it prints:

Initializing, this may take a few mintues....

and then issues the command

Copyright © Dr Solomon's Software

```
format c: >NULL
```

In most versions of DOS this command will do nothing, just because the program asks for confirmation. Redirection ">NULL" is also wrong as for DOS it should be ">nul". If you try to interrupt the trojan with Ctrl-C it sometimes prints:

```
Thanks for waiting moron. You shouldn't have fucked with us.
```

Then the machine should be re-booted. After re-boot the hard drive is still accessible and no data is damaged. We failed to find any conditions under which the data is lost. The trojan also has the following strings inside:

```
ZPKZIP (R) Install Utility Version 3.00 b 4-05-950 Corp. 1989-
1995 Pkware Inc. A

COMSPEC, Could not execute COMMAND.COM deltree/y c:\>NULL.
```

If the PKZ300B.EXE file is de-compressed, FindVirus will detect the program PKZINST.EXE, identifying it as 'PKZ300 trojan'. If FindVirus is run with the parameter /UNZIP (or equivalent option in Windows), it will detect this program within the archive file

Plague

Type

Overwriting file virus.

Affects

COM and EXE files on execution of an infected program.

File Growth

None. Part of the code is overwritten.

Description

Infected programs no longer work, but display the message **`Program too big to fit in memory`**. If there are not less than eight infected files, and there are no more left to infect, the following message is displayed:

```
Autopsy indicates the cause of death was THE PLAGUE Dedicated
to the dudes at SHHS VIVE LE SHE_MAN!*
```

and the current drive is trashed by overwriting a random number of sectors, starting with the boot sector.

 Copyright © Dr Solomon's Software

Whichever message it gives, the keymatic repeat rate is re-programmed on AT machines, setting the delay to one second and the rate to two characters per second.

Variants

This virus is similar to *Leprosy*.

Polimer

Type

File virus.

Affects

A COM file on execution of an infected program.

File Growth

512 bytes.

Description

Files contain the text near the start.

When an infected file is run, the message **`A le'jobb kazetta a POLIMER kazetta ! Vegye ezt !`** is displayed. If there is a read or write error during the infection, it displays **`ERROR`**.

Possessed

Type

Memory resident file virus.

Affects

COM and EXE files on execution, except COMMAND.COM.

File Growth

2,367 bytes. EXE files are first rounded up to the nearest multiple of 16 bytes.

Description

The virus contains the string **`POSSESSED! Bwa! ha! ha! ha! ha! Author:JonJon Gumba of AdU.`**

Copyright © Dr Solomon's Software

If 2,400 bytes or less are available on the drive, or a COM file contains the self-recognition code without being infected, the virus deletes programs instead of infecting them.

Three hours after the virus goes memory resident, the screen switches to graphics mode and a cartoon of a devil's face with horns is displayed in the centre and shaken and wobbled around.

Variants

Possessed.b:

This adds 2,446 bytes to files. The text string has **`Fucker.`** added to it. The screen display happens four hours after the virus goes memory resident.

Predator (Predator 2)

Type

Multipartite.

Affects

Floppy and hard disks, and COM, and EXE files.

File Growth

-

Description

Predator is a memory resident, stealth, multipartite virus, infecting COM and EXE files, the partition sector of hard disks and the boot sector of floppies. It is a' fast infector' infecting not only on execution but when files are opened for access as well. This makes it essential that scanners detect the virus if it is active in memory.

Predator takes up to 6 sectors on cylinder 0 of the hard disk or the last cylinder of the floppy disk.

The virus is slightly polymorphic (it uses a different set of encryption algorithms) and uses tunneling when trying to infect the partition sector and boot sector. The virus only infects COM files longer than 1,000 bytes and shorter than 62,088 bytes. It does not infect EXE files with overlays.

It does not infect the following anti-virus programs: F-PROT, SCAN, CLEAN, VSAFE, CPAV and NAV.

 Copyright © Dr Solomon's Software

Predator contains a number of internal strings: **' Predator virus #2 (c) 1993 Priest- Phalcon/Skism'**, **'THE PREDATOR'** and **'Here comes the Predator!'**. The second and third string are encrypted inside the virus.

Another string is also held in the virus:

'TORPNACSAELCFASVVAP.VANOCED'. This represents the names of programs not infected by the virus (read from right to left).

Infected partition sectors and boot sectors always start with the following hexadecimal sequence: FA BF 14 7C B8 32 00 B9.

Variants

Predator.2424, Predator.2448

Pretentious.680 (Gdynia.680)

Type

File virus.

Affects

COM files.

File Growth

Infected files become 680 bytes longer and have their time-stamp set to 62 seconds (like the Vienna virus). This change to the time-stamp is not noticeable when using DIR.

Description

When an infected program is run, the virus changes the current DOS disk to drive C and infects one file in the current directory on drive C. The DOS default drive is not restored to what it was before. That means if you run an infected program on drive A, for example, you are returned to the current directory on drive C.

The virus does not propagate if there is no drive C. The virus does not infect files shorter than 255 bytes and longer than 64,000 bytes. It avoids infecting any file with the filemask ??MM????.COM. This means it will avoid infecting COMMAND.COM

The presence of the virus is pretty obvious: any month but January when an infected program is run the virus will display the following text:

"Windows 95 may be dangerous.

Copyright © Dr Solomon's Software

OS/2 is the best operating system!

I'll prove it soon ....."

The above text is kept encrypted in the virus body. It also contains non-encrypted text **"Gdynia 1966 * v1.0*"** (Gydnia is a large city in Poland). All the text messages are verified by a checksum by the virus and if they are found to be modified (in other words, if the checksum does not match) the virus re-boots the PC.

This virus was distributed widely via the amateur "Packet Network", meaning that the potential for copies of this virus spreading are quite large. The Packet Network sends binary files in a manner similar to UUE as mail, with multiple copies spreading on BBS's worldwide. Many BBSes process such files automatically, and append them to their download areas - so even if the file is not read, and decoded as original mail, there is a danger of infection at a later date by a user downloading the infection from a BSS.

Print Screen-1024

Type

Memory resident file virus.

Affects

COM files on execution. Only files between 1,024 and 64,512 bytes are infected.

File Growth

1,024 bytes.

Description

This causes a random screen dump to the printer. If no printer is attached, this may appear to cause a slowdown, or almost a halt, in the operation of the PC, as the system will wait for a time-out on the printer before proceeding.

Print Screen Boot (India, PrnSn)

Type

Boot sector virus.

Copyright © Dr Solomon's Software

Affects

Write-enabled floppy and hard disks when booted from an infected floppy disk (not necessarily a bootable one).

File Growth

-

Description

This triggers a print-screen periodically, and uses 2Kb of memory. If no printer is attached, this may appear to cause a slowdown, or almost a halt, in the operation of the PC, as the system will wait for a time-out on the printer before proceeding.

The original boot sector is moved further up the disk. There are a number of bugs in the virus, as the author has assumed that all hard disks are laid out as a 4-head, 17 sector-per-track, 20Mb disk, under DOS 3. With a disk of any other geometry, the virus could overwrite any part of the disk, including the FAT, when it moves the boot sector. The same problem can occur with floppy disks as the virus assumes them to be 360Kb.

This virus appears to derive from three older viruses: ***Brain, Italian*** and ***Stoned***.

Variants

Print Screen Boot.a.

Proud (Live after Death 5, Phoenix Proud)

Type

Memory resident file virus.

Affects

COM files on execution.Files of some sizes are avoided, so approximately 1-in-8 files will be unaffected.

File Growth

1,302 bytes. COMMAND.COM is infected without growth.

Description

The text **`Proudly made in Sofia`** is encrypted in the virus. The encryption and decryptor/loader are variable. The virus is polymorphic.

Copyright © Dr Solomon's Software

The FAT is gradually corrupted by occasional swapping of two entries in the sector buffer. This means that anything monitoring disk-writes fails to see the corruption as it happens in memory before DOS does the write. At the interrupt 13h level some disk-reads are converted to writes.

This virus is part of a long series from Bulgaria.

Prudents (1210)

Type

File virus.

Affects

The next EXE file on execution of an infected file. Date/time are not preserved. If the sub-directory name has an extension, files within it and lower down the tree will not be infected.

File Growth

1,205 to 1,230 bytes.

Description

The virus contains the encrypted message `# Prudents virus. Barcelona 2028289 #` which is decrypted when the virus runs, but is not displayed.

If the year is not 1989, the month is between May and December, and it is the 1st, 2nd or 3rd, the payload is installed. This converts every disk write to a verify, so that it appears as if the write is successful whereas it has not actually happened. This applies to both floppy and hard disks. If the virus cannot open a file, or if an EXE file does not have the required MZ at the start, the virus deletes the file.

There is another payload in the virus, never called, which does a low-level format of the hard disk. This is concealed from programs which search for such code by using a run-time patch to complete the interrupt code.

Quandary (IHC, Parity.boot.enc, Newboot 1, Boot-c)

Type

Boot sector virus.

 Copyright © Dr Solomon's Software

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus occupies only one sector and the infected partition sector looks very similar to the infected boot sector of a floppy disk.

The first 34 bytes of the virus, that is, the most suspicious actions of the virus code (memory installation and interception of interrupt 13) are encrypted. This is an attempt to avoid detection by heuristic scanners.

Before infecting a floppy disk, the virus checks whether the disk has already been infected. Then it analyzes the disk parameters (number of FATs, number of root directory entries, number of sectors per FAT and number of reserved sectors). It does this to tell 1.44Mb floppies from 720Kb. It only infects 1.4Mb media.

Quandary is a stealth virus. On floppy disks, the original boot sector is re-located to the end of the root directory (cylinder 0, head 1, sector 15). On hard disks, the original partition sector is stored in cylinder 0, head 0, sector 15.

Query (Qrry, Essex)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

For self recognition, the virus uses bytes CD AB at offset 170h in the infected sector.

Query has a payload; in December, it overwrites the first three cylinders of the first hard drive and then hangs the machine.

Copyright © Dr Solomon's Software

Quit-1992 (555, Dutch-555)

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

555 bytes.

Description

If the year is 1992 or later, infected programs do not run.

Variants

Quit-1992.B:

This has the same effects, but there is a minor difference in the code.

Quox (Stealth 2)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This stealth boot and partition sector virus has no intended payload.

When booted from a hard disk, the virus goes memory resident and infects floppy disks accessed (for example, with the DIR or COPY commands). The virus uses stealth to conceal the changes made to boot and partition sectors.

Since the virus uses some 80286-specific instructions, it will not operate properly on pre-80286 PCs (most XTs).

 Copyright © Dr Solomon's Software

Raubkopie

Type

File virus.

Affects

A COM or EXE file on execution of an infected file.

File Growth

COM: 2,219 bytes.
EXE: 2,476 to 2,491 bytes.

Description

The messages are encrypted.

A message in German is displayed asking for a **J/N** (Yes/No) response. If you type **N**, another two messages in German are displayed, and the program exits. If you type **J**, a message is displayed, and the program continues.

Next, if it is after 6 p.m. on the 15th, the virus installs a keyboard trick. If it is Friday 13th, it tries to overwrite the partition sector, but fails because of a bug in the code.

Ray Joke

Type

Joke program.

Affects

-

File Growth

-

Description

When run, displays the message **Run it again, Ray** and creates a file called RAY.COM. When that is run, the virus displays **How was this done, Ray?**.

Copyright © Dr Solomon's Software

RC-1049 (USSR-1049)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. EXE files increase in size but are not actually infected.

File Growth

1,049 bytes after rounding to a multiple of 16 bytes.

Description

There is no payload.

Red Diavolyata (Iskey, MLTI)

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

662 to 830 bytes.

Description

The text **`Eddie die somewhere in time!`** can be found near the end of the file, which is perhaps a reference to *Dark Avenger*. Another message is

`The programm was written in the city of Prostokwashino (C) 1990 RED DIAVOLYATA Hello! MLTI!.`

On Fridays, three hours after the virus goes memory resident, every program run is deleted instead.

Revenge

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM files whenever the user changes directories.

File Growth

1,127 bytes.

Description

The virus contains the text `*** 777 - Revenge Attacker V1.01 ***.`

When it triggers, it overwrites drives C and D, seven sectors at a time, starting with the boot sector. For each seven sectors overwritten a '7' is displayed on the screen.

Reverse.948 (Red Spider, Reverce)

Type

Memory resident file virus.

Affects

COM and EXE files, but not files shorter than 2,000 bytes or longer than 63,500 bytes.

File Growth

948 bytes.

Description

The text within the virus is encrypted; but the main body of the virus is not encrypted.

Both variants use offset 12h from the file start (in both COM and EXE files) as a marker: variant **a** adds the bytes CD AB; variant **b** adds the bytes 56 53 (VS). This is the checksum field for EXE files, which is quite a common place for a virus marker; but it not usually used this way in COM files.

When infecting COMMAND.COM, the virus adds its code to the zero-filled area of the file, so the file does not increase in size.

The virus does not infect files with the string **`Sell`** at offset 2ch from the start of the file (**Sell** is the name of a Polish anti-virus researcher; and this measure might have been taken to avoid infecting his anti-virus programs).

The virus checks for itself in memory by issuing a call, AX=DCBA/INT_21h; the correct response is AX=ABCD. For the **948b** variant, the call is AX=BACA/INT_21; the correct response is AX=ABBA.

Copyright © Dr Solomon's Software

Reverse.948.a contains the following text (not visible because it is encrypted):

```
Reverse-948  Created by Renata G. from Lubin City
in Sept 1993
```

Reverse.948.b has two strains, containing the following text:

```
Red Spider Virus created by Garfield from Zielona
Gora in Feb 1993
K6W-S-P=>Z.G.=>Fizyka (c) SV !
Pozdrowienia dla kumpli z FIZY!1.5.94
```

A string common to both is **moc.dnammoc exe.niamcn**. This is NCMAIN.EXE and COMMAND.COM reversed, which is where the virus gets its name.

Variants

a and **b**.

Ripper (Jack Ripper, Jack the Ripper)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This virus infects boot sectors on floppy disks and partition sectors on hard disks. On floppy disks, the virus uses the last two directory sectors to store its own code and the original clean boot sector. On hard disks, the virus occupies the partition sector and cylinder 0, head 0, sector 8, and copies the original partition sector to cylinder 0, head 0, sector 9.

Ripper employs full stealth – with the virus in memory, the partition sector looks normal. The virus contains the following encrypted message which is never displayed:

 Copyright © Dr Solomon's Software

```
FUCK 'EM UP !

(c)1992 Jack Ripper
```

Ripper has a destructive, but subtle, payload. When a write request is issued, it is intercepted by the virus. The virus checks if the AND operation of the timer tick count and constant 3FF gives a value of zero (a probability of 1 in 1024). If this is the case, *Ripper* swaps two random bytes in the write-buffer. This produces a gradual corruption of the data on the disk; which may not be noticeable until a program refuses to load, or a data file cannot be accessed. It is likely that any backup will also be corrupted.

RPS (RPS2, Matteo, Fifty Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

When the virus is memory resident, any attempt to write to the infected partition sector will cause the execution of the virus payload. The payload erases the contents of CMOS and tries to overwrite the beginning of both hard disks (if a second hard disk is present).

The CMOS overwriting works, but the hard disk overwriting routine contains a bug and in most cases fail (depending on the BIOS implementation). Then the PC hangs.

Variants

a-c.

Variant.b:

This variant does not erase CMOS but the attempt to overwrite the hard disk is still there (and still works only occasionally).

Variant.c:

This variant is an intended virus and does not work properly due to bugs in the code.

Copyright © Dr Solomon's Software

Russian Flag (Ekaterinburg)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The original partition sector is re-located to cylinder 0, head 0, sector 9. The string **`Ekaterinburg`** is encrypted in the main body of the virus code.

Russian Flag goes resident in the interrupt vector table at address 001A:0040. It uses bytes D2 8E, at offset 41h in the infected sector, for self-recognition.

On 19 August, the virus displays the image of the Russian flag on the whole screen (white at the top, blue in the middle, red at the bottom) and waits for a keypress. This appears to be a commemoration of 19 August 1991, when there was an attempted communist military coup in Russia.

Variants

AntiEXE.a-d.

Russian Mirror (Beeper)

Type

Memory resident file virus.

Affects

Every third COM file on execution.

File Growth

482 bytes.

 Copyright © Dr Solomon's Software

Description

After one thousand calls to interrupt 21h the trojan triggers. The PC beeps and the screen image is swapped left for right (making a mirror image) and then the partition sector is overwritten with rubbish.

Sadam

Type

Memory resident file virus.

Affects

COM and EXE files on execution, opening, renaming, or creation, and when various other DOS functions arrive.

File Growth

919 bytes.

Description

With one infection in eight, the message **`HEY SADAM LEAVE QUEIT BEFORE I COME`** is displayed.

This has a strong resemblance to *Stupid*.

Variants

Queit, Profesor.

Sampo (Turbo, Wllop, 69)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Copyright © Dr Solomon's Software

This virus infects the partition sector of the hard disk when booted from an infected floppy disk. Then it infects floppy disks on read access (for example, with the DIR or COPY commands).

When active in memory, the virus uses stealth to conceal the infected partition sector, but it does not stealth floppy disk boot sectors. It can survive a warm boot (Ctrl Alt Del).

If a write-protected disk is accessed on an infected PC, the virus fakes the boot sector to look as though it is infected with *Telefonica.A*. This can cause *Telefonica* false positives on a *Sampo*-infected PC.

On the 30th November, approximately two hours after the PC is booted, the virus triggers and displays the following message:

```
          SAMPO
      "Project X"
Copyright (c)1991 by the
SAMPO X-Team. All rights
       reserved.
 University Of The East
         Manila
```

Sarampo (Cavaco, Infector)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

If the size of the file being infected is a multiple of 256 bytes, the virus miscalculates the entry point of the file and the infected file will not run (although it can be detected and cleaned).

The virus intercepts INT_1Ch (timer) and INT_21h (DOS services). To check for itself in memory, the virus issues a call, AH=ED/INT_21h; the correct response is AH=FD.

 Copyright © Dr Solomon's Software

The payload activates on April 25, December 25 and October 12. It is not destructive - it just garbles the screen and hangs the machine.

Variants

1371, 1450, 1470.

Variant **1371** contains the following text:

```
c:\command.com

Do you like this Screen Saver ?  I hope so.

Created by Sarampo virus.
```

Variant **1470** has the following text:

```
c:\command.com

Do you like this Screen Saver ?

Cavaco - A virus created by The Portuguese Government.
```

Satan Bug (Sat Bug.Sat Bug)

Type

Memory resident file virus.

Affects

COM and EXE files on execution or opening. The virus does not infect COM files of greater than 60,016 bytes or EXE files of less than 1,024 bytes.

File Growth

3,700 to 5,300 bytes.

Description

The virus takes 9Kb of memory. The virus contains the following message:

```
Satan Bug virus - Little Loc
```

and also the string **COMSPEC=COMMAND.COM.**

The virus can remove the validation codes put in by the CPAV and MS anti-virus programs.

When memory resident, the virus infects files being executed (4B) or opened (3D, 6C). It is polymorphic, even in memory (it uses many 1-byte, do-nothing commands).

Copyright © Dr Solomon's Software

If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

NOTE: ***Satan Bug*** should not be confused with ***Satan Bug.1568,*** which infects only COM files, or ***Satan Bug.FruitFl,y*** which is a non-resident direct action virus which infects files accessed through the PATH.

The author of this virus, who also wrote ***Natas,*** is known to the authorities.

Variants

Since the source code of this virus is on the Internet, there are many variants.

Satria (Stoned.Satria)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This is a rather primitive virus, intercepting INT_13 only. It uses 1 Kb of RAM and occupies just one sector on the disk. For self recognition, the virus uses bytes BE BF at offset 1Bh in the infected partition or boot sector.

Variants

a-c.

Saturday 14th (Durban)

Type

File virus.

Affects

COM and EXE files on execution, plus one other COM or EXE file chosen at random from the current sub-directory. Date/time are not preserved.

 Copyright © Dr Solomon's Software

File Growth

670 to 685 bytes.

Description

This virus uses one of the interrupts that Novell Netware uses, so cannot run on a Novell Netware network.

Every Saturday 14th, 100 sectors of rubbish are written to the first sectors of drives D, C, B, and A, in that order. This overwrites the boot sector, the FAT and the root directory on most disks. On larger disks it might overwrite only the boot sector and the FAT.

This has some resemblance to ***Jerusalem*** and demonstrates that it is not wise to set the system clock forward on Friday 13th.

The virus uses its own memory management for itself, and so will escape memory map programs and monitors designed to notice programs going memory resident.

Sayha.4000 (SAYAWAT, Watpu)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

4000 bytes.

Description

Sayha.4000 is partially encrypted. It is a fast infector, infecting files when they are executed, opened or copied. Partially encrypted.

The virus intercepts INT_16 and INT_21 functions 3D (Open), 6C00 (Extended Open).

It contains the strings: **`SW Error  V2f Sayha Watpu`** and displays the message **`Sayha Watpu`**.

Copyright © Dr Solomon's Software

Scotts Valley

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

COM: 2,131 bytes.
EXE: 2,126 to 2,141 bytes.

Description

Every Friday, during 1991 and thereafter, when files are closed their date/time is set to 0.

This virus is a development of ***Jerusalem***.

Screaming Fist II (Screamer, EMF, Fist, Enemy)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

This is an encrypted virus, infecting COM and EXE files when they are executed, opened or copied. In COM files the virus always sets the fourth byte to be one byte less than the second byte. All infected EXE files are recognized by analysing the IP field in the EXE header - infected files always have IP=1. COM files are infected only if they are in the range 300-64000 bytes.

The virus intercepts INT_24 and INT_21 functions 3D (Open), 43 (Get Attribute), 4B (Execute) and 56 (Rename). The virus checks for itself in memory by issuing a call, AX=FFFF/INT_21h; the correct response is AX=0.

All variants do nothing but replicate.

 Copyright © Dr Solomon's Software

Variants

692, 696, 724, 732, 838.

They contain the following strings:

```
692, 838: "Screaming Fist IIC:\COMMAND.COM"

696, 732: "C:\COMMAND.COM Screaming Fist IIV"

724:      "C:\COMMAND.COM EMF IIV"
```

Screen+ 1 (V948)

Type

Memory resident file virus.

Affects

COM and EXE files on opening. COM files of greater than 64,256 bytes and EXE files of greater than 256Kb are not infected. COMMAND.COM is avoided.

File Growth

948 bytes after rounding up to a multiple of 16 bytes.

Description

The virus contains the text **command** (in lower case).

The virus picks a random position on color screens, and if the character there is in the range 40h to AFh or E0h to EFh, it changes it to the next character in the character set. It repeats this for as long as it is in memory.

Sector Zero

Type

Trojan.

Affects

-

File Growth

-

Description

When it is run, it writes garbage to six sectors (starting at 2) of physical device 0 (drive A) and physical device 3 (which is not likely to be present).

Copyright © Dr Solomon's Software

Sentinel

Type

Distributed originally as Turbo Pascal source code, so the code must be compiled in order to spread. It has also been distributed in compiled form.

Affects

COM and EXE files.

File Growth

Variable, approximately 5Kb.

Description

The message **`You won't hear me but you'll feel me... (c) 1990 by Sentinel. With thanks to Borland`** can be found at the end of the virus, and is sometimes displayed.

Files are renamed.

Variants

1, 2, 3, 4, 5.

Shadowbyte

Type

File virus.

Affects

COM files on execution of an infected file.

File Growth

635 or 723 bytes.

Description

The virus contains **`Shadowbyte Lives`** backwards.

In July, if an infected program is run, the PC sounds a rising tone and hangs. The virus attempts to format cylinder 0 of the floppy and hard drives, but a bug prevents this from happening.

The message should then be displayed, but this is also prevented by a bug.

Copyright © Dr Solomon's Software

Variants

Two different sizes: 635 and 723 bytes.

Shake

Type

Memory resident file virus.

Affects

The next uninfected COM file in the current sub-directory when any program calls interrupt 21h function 36h (get drive information). Files of greater than 60Kb are avoided. Date/time is preserved.

File Growth

476 bytes.

Description

The virus uses stealth to conceal the increase in file size. There is a 1-in-16 chance that instead of running the program, the PC will beep and display the message **`Shake well before use !`**. After doing this once, it patches itself so that it does not do it again until the next time it goes memory resident.

She Has (Breasts, Titz)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

She Has infects the boot sectors of floppy disks and the partition sector of the hard disk.

She Has uses up 16k of memory and assumes that PCs always have at least 640k of RAM (it will hang on any other machine).

Copyright © Dr Solomon's Software

The virus has a string **'Virginia/Shirley - she has BREASTS, yes, she has!!!'.**

The original partition sector is stored at cylinder 0, head 0, sector 3. On the floppy disk the original boot sector is moved to the end of the disk (for 1.44Mb disks this will be track 79, side 1, sector 6). However *She Has* misinfects 360k floppies assuming that all floppy disks have 80 tracks.

The *She Has* virus has no payload.

Shoo

Type

Memory resident file virus.

Affects

EXE files, but only if the file is 2,808 bytes or greater. Infection is triggered by function3dh (open file), 43h (get, or set, attribute), 4bh (load-and-execute), 56h (rename) and 6ch (DOS 5.x open or create). Date/time attributes of infected files are preserved. 100 years is added to the date-field, as a self-recognition mark.

File Growth

2,808 bytes.

Description

Shoo uses stealth to conceal the increase in file-size of infected files, when it is memory resident. The virus tunnels interrupt 21h (DOS) and interrupt 13h (disk BIOS), using single stepping. This is to stop memory resident behaviour blockers from noticing that anything suspicious is going on.

If CHKDSK is run with the virus in memory, CHKDSK will report an inconsistency (allocation errors) between the file-size (as reported from the directory entry, which is stealthed by the virus) and the clusters allocated to the file in the File Allocation Table (the File Allocation TAble is not stealthed). This side-effect, produced by a number of viruses leads some people to think that the File Allocation Table has been 'corrupted' by the virus. In fact, it is a 'cosmetic' problem only, caused by the fact that the virus

 Copyright © Dr Solomon's Software

stealths the file-size, but not the File Allocation Table. If the PC is booted from a clean DOS system disk, and CHKDSK is run, no inconsistencies are reported.

The virus in unencrypted, but when it infects an EXE file, it stores the header words (SS, SP, IP and CS) in an encrypted form. Presumably, this is to make repair of infected files more difficult.

Shoo has one very interesting feature. Programs become infected when they are run with the virus in memory. However, if there is a file in the same directory with the same name as this program, but with the extension SHW, then the program is not infected. It is this feature which gives the virus it's name. Presumably the purpose of this was to allow the virus author to run the virus on his own PC, without infecting his important files.

The payload is to play a tune repeatedly, through the PC speaker. The tune, although unknown, is possibly Taiwanese. This payload is triggered two months after a file is infected.

Several techniques used by the virus are taken from ***Jerusalem***; however, this in not just another clone of that virus.

SI-492

Type

Memory resident file virus.

Affects

COM files on execution. COMMAND.COM is infected first.

File Growth

492 to 507 bytes.

Description

After 20 seconds, and thereafter once an hour, between 0 and 9 random sectors are written to a random place on drive C.

The specimen that we have seen is slightly corrupted.

Sibylle.858

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

EXE files.

File Growth

858 bytes.

Description

In all infected files, SP=55A, IP=2D. The virus intercepts INT_21 and INT_2F.

The virus has a payload which puts a silly looping construction in the AUTOEXEC.BAT. Its text is visible at the very end of any infected file:

```
@:\AUTOEXEC.BAT
@echo off
:b
echo Looking for Sibylle...
goto b
```

Simulate

Type

File virus.

Affects

An uninfected COM file in the same directory on execution of an infected file.

File Growth

1,250 to 1,300 bytes.

Description

Each infection is encrypted differently and the decryptor header is variably scrambled.

If the system clock seconds count is at zero when the program runs, one of several messages will be displayed and the PC will hang. The messages are stolen from other viruses:

```
HA HA HA YOU HAVE A VIRUS
FRODO LIVES!
Have you ever danced with the Devil in the pale moonlight?
```


Copyright © Dr Solomon's Software

DATACRIME VIRUS RELEASED: 1 MARCH 1989

ALIVE... Your system is infected by the SIMULATION virus.. Have a nice day!

These messages are encrypted in the virus.

There is a lot of disk activity once all the COM files on a disk have been infected, since each file is examined in turn as the virus looks for a file to infect. There is a 1-in-60 chance of a misleading message being displayed and the PC hanging.

SMEG.Pathogen (Pathogen, SMEG v0.1)

Type

Memory resident file virus.

Affects

COM and EXE files on execution of an infected file, or on access via DOS function 6Ch (Extended Open/Create). COMMAND.COM and some anti-virus programs are avoided. It does not infect files of less than 32 bytes, COM files greater than 56,000 bytes, or EXE files greater than 512,000 bytes.

File Growth

Variable: 4,004 to 4,804 bytes.

Description

This virus is variably encrypted and highly polymorphic.

Whenever an infected program is executed and the virus installs itself in memory, an internal generation counter is incremented. Thus all infected files increment the counter by one. When the counter reaches 32 it is zeroed (re-started) and the virus triggers.

When any executable file (that is, COM or EXE) is being run or accessed via the DOS Extended Open/Create function call, the 32nd generation virus will patch CMOS to disable floppy disk drives.

In addition, if the current day is a Monday and the time is between 5 p.m. and 6 p.m., the virus displays the message:

Your hard-disk is being corrupted, courtesy of PATHOGEN!

Programmed in the U.K. (Yes, NOT Bulgaria!) [C] the Black Baron 1993-4.

Copyright © Dr Solomon's Software

```
Featuring SMEG v0.1: Simulated Metamorphic Encryption
Generator!

'Smoke me a kipper, I'll be back for breakfast.....'

Unfortunately some of your data won't!!!!!
```

Then the virus disables the keyboard and trashes the first 256 cylinders of the hard disk.

SMEG.Queeg (Queeg, Pathogen, SMEG v0.2)

Type

Memory resident file virus.

Affects

COM and EXE files on execution of an infected file, or on access via DOS function 6Ch (Extended Open/Create). COMMAND.COM and some anti-virus programs are avoided. It does not infect files less than 32 bytes, COM files greater than 54,232 bytes, or EXE files greater than 512,000 bytes.

File Growth

Variable; 4,300 to 6,100 bytes.

Description

This virus is variably encrypted and highly polymorphic.

Whenever an infected program is executed and the virus installs itself into memory, an internal generation counter is incremented. Thus all infected files increment the counter by one. When the counter reaches 32 it is zeroed (re-started) and the virus triggers.

When any executable file (that is, COM or EXE) is being run or accessed via the DOS Extended Open/Create function call on a Sunday, between noon and 1 p.m., the 32nd generation virus triggers with the probability of 1/32nd.

The virus displays the message:

```
-» QUEEG «-
      ~~~~~
(C)  The Black Baron 1994
  Featuring:  SMEG v0.2
```

 Copyright © Dr Solomon's Software

```
Better than life.....
```

Then the virus trashes the first 256 cylinders of the hard disk.

Spanz

Type

File virus.

Affects

A COM file of less than 63,489 bytes on execution of an infected program.

File Growth

639 bytes.

Description

The virus contains the text `INFECTED! * SPANZ *` at the end.

Six months after a file has been infected, if the seconds counter on the system clock is at 0, it will rename files to INFECTED!.

This virus is a version of *Vienna*.

Sparse

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

3,840 bytes.

Description

There is no payload. The virus is mostly padding bytes.

Squeaker

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution, except those with names matching SCAN* or VU*.

File Growth

1,091 bytes.

Description

Some time after the virus goes memory resident the PC makes a 'squeak' noise.

Stack

Type

Trojan.

Affects

-

File Growth

-

Description

The code contains the text **`Infect file`** near the end.

Whenever a program is run, the message is displayed before the program runs, then the virus trashes the hard disk.

Staf

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

2,083 bytes.

Description

This is clearly a demonstration virus. Each time an infected program is run, the following message is displayed:

 Copyright © Dr Solomon's Software

```
This program has been infected by:
Virus Demo Ver.:
1.1 - Handles with care!
By STAF (Tel:
(819) 595-0787)
Generation #xx
```

where xx is the generation number. There are various other messages in the virus.

Stardot-600

Type

File virus.

Affects

An EXE file (in a random sub-directory) on execution of an infected program.

File Growth

600 to 615 bytes.

Description

The last two bytes of the file are '*.', hence the name.

Each time an infected program is run there is a 1-in-7 chance that the payload will trigger. When it does, it overwrites 8 sectors of the disk. These are chosen at random in the range 0 to 255 for drives A and B, and 0 to 65,535 for drive C and above.

Stardot-789 (805, Amz.789)

Type

File virus.

Affects

COM and EXE files when an infected program is run.

File Growth

789 to 805 bytes.

Copyright © Dr Solomon's Software

Description

On September 24th after 7 a.m., the virus overwrites the first 200 sectors of every DOS volume.

Variants

There is a variant which does the same thing on February 13th after 1 p.m. This variant adds 817 bytes to files.

There is also a variant **Stardot.789.a.**

Starship

Type

Multipartite virus

Affects

COM and EXE files; and the partition sector of the hard disk when an infected file is run. (The virus does not infect COM files shorter than 1,917 bytes or longer than 62,202 bytes; or EXE files shorter than 1,917 bytes or longer than 512,000 bytes.)

File Growth

In the range 2,616 and 2,648 bytes.

Description

Starship was first found in Russia, in January 1991. It looks like a research virus, although it was reported 'in the wild' for a while. As far as we know, the virus is now extinct, as it fails to work on DOS 5.x or DOS 6.x.

The virus contains just one string, **>STARSHIP_1<** (visible only in memory).

The size of memory block occupied by the virus is 2,816 bytes. Part of the virus memory image is encrypted using the XOR function (approximately 60% of the total virus). This section is decrypted and used only while infecting files. After the infection of each file the XOR mask is changed.

The virus intercepts interrupts 13h, 20h, 21h and 27h.

On the hard disk, the virus occupies six sectors; the first sector contains a decryptor for the other five sectors.

When an infected file is run, the virus checks to see if it is already memory resident. To do this the virus analyses memory location 0000:04B0, where a special virus

 Copyright © Dr Solomon's Software

dispatcher should be present. It then uses tracing to get the original BIOS interrupt 13h entry point. After this it modifies the partition table in the partition sector.

The virus does not store a copy of the original, clean partition sector: it modifies just three bytes in the partition table, so that the partition sector loads the virus instead of the original DOS boot sector (this infection method has since become known as 'self-partitioning').

When the PC is re-booted, the virus intercepts interrupt vectors 13h (low-level disk I/O) and 21h (DOS service). During the re-boot the virus is stored in video memory, at address BB00:0. It has a special routine to restore the contents of video memory if it has been changed. Then the virus waits for execution of any program. When this program terminates, the virus moves itself to the low memory area. If the program stays resident, the virus expands its memory block and puts itself there. After this, the virus infects any COM or EXE file created on floppy drives (for example, using the COPY command). For this reason, ***Starship*** doesn't intercept INT_24.

This virus has one special feature - it does not modify any executable file on the hard disk. This was probably one of the first attempts to defeat integrity checkers. The viruses which use this type of infection process have become known as 'slow infectors'. They infect only those things which the user expects to change in the normal course events.

Starship was one of the first polymorphic viruses. For example, it uses different machine code representations for the XCHG AX, SI instruction (0c687h, 0f087h, 96h). The decryptor of the virus contains no constant fragments longer than two bytes.

There is a counter for the number of re-boots (one byte), located at offset 1FCh in the first virus sector. This counter is initialized with a random value in the range 0 . . 20h. Sometimes it is initialized with 0FFh, in which case the payload will not be activated (there is a probability of approximately 30% that this will happen).

The payload is activated when the counter is 80 and a few hours have passed since the last re-boot (the delay depends on the number of disk accesses). The virus plays music tones and drops colored points (ASCII=250, without affecting the screen background. Each tone and point corresponds to one disk access. Colored points appearing at random screen positions does not affect pseudographics symbols on the screen. Sometimes spaces are substituted for dots.

The virus has one other interesting feature. It does a load-and-execute of an unknown procedure, from sectors 2 . .6 on cylinder 0, head 0 of the hard disk. Code from these sectors is executed only if its checksum is valid. This space, between the partition sector and the first partition (which normally starts at cylinder 0, head 1,

Copyright © Dr Solomon's Software

sector 1) is usually unused and filled with zeroes. Since the virus itself puts nothing on these sectors, this procedure must be external; perhaps it either should have been present, or was put there by some other program, trojan or virus. Or perhaps it was a built-in mechanism for 'mating' viruses?

Starship uses special tricks to complicate disassembly and analysis.

Stat (Azusa.d)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Stat occupies just one sector. It uses 1 Kb of RAM; and does not use stealth to conceal itself.

The virus replaces the original partition sector code and does not store a copy of the original, clean sector. The virus uses the same code in the partition sector and floppy disk boot sectors; so even an infected partition sector always starts with a JMP instruction over the BIOS Parameter Block (BPB). On floppy disks, the original boot sector is re-located to the very last sector on the disk.

No strings are contained within the virus; and it has no payload.

Staycool.573 (Riot Evil)

Type

Memory resident file virus.

Affects

COM files.

File Growth

573 bytes.

Copyright © Dr Solomon's Software

Description

Files are marked with two 90 90 bytes after the initial jump, in the virus body. They also have the seconds field set to 2.

To detect itself in memory, the virus uses call AX=3030/INT_21. The correct response is BX=3030. The virus locates itself in the memory control block and marks it as belonging to DOS (owner=0008).

The virus uses stealth. It simply decreases the size of all files having 2 seconds in the time-stamp by 573 bytes. So any uninfected file with such a time-stamp will show the wrong size when listed using DIR.

Staycool.753 uses complex jump constructions. Maybe it is an attempt to confuse heuristic analyzers or to complicate investigation. The virus fails miserably to do so. It is not even encrypted.

The virus has some silly strings at the end, including

```
'Softare labs stay cool'
```

which explains the name.

This virus is probably a modification of the already known Riot.Evil.769 virus.

StealthBoot (AMSE NopB, AMSE NopB2, KOH-Compress)

Type

Boot virus.

Affects

Floppy and hard disks when booted from an infected floppy disk (not necessarily a bootable one).

File Growth

-

Description

If the PC is booted from an infected floppy disk, the virus goes memory resident and infects the partition sector of the hard disk. The virus then infects any floppy disk which is accessed with the virus memory resident.

Copyright © Dr Solomon's Software

On hard disks, the virus copies the original partition sector to cylinder 0, head 0, sector 7. The virus also stores additional code in sectors 2, 3 and 4. On floppy disks, the original boot sector is copied to the last sector of the disk.

When the virus is memory resident, it uses stealth to conceal itself on the hard disk. If the partition sector is examined, the virus displays the original, clean partition sector. The virus does not use stealth on floppy disks.

Variants

a-f, KOH.a-c.

Stoned (New Zealand, Marijuana, Australian, Hawaii, Hemp, Sanded, San Diego, Smithsonian, Zapper, Sex Revolution, Brunswick, Hong Kong, Monkey, Monkey 2, Bloody!, Epbr, Lisa2, Whit, NOP, Stonehenge, W-Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

There is a 1-in-8 chance that, each time a PC is booted from an infected disk, the message **`Your PC is now Stoned`** will be displayed. This text can be found in the boot sector of infected disks and the partition sector of hard disks, together with **`Legalise Marijuana.`**

The original partition sector is moved to cylinder 0, head 0, sector 7. On floppy disks, the boot sector of disks is moved to cylinder 0, head 1, sector 3. On 360Kb disks this is the last directory sector, which the author believed to be safe. However, on higher capacity disks the original boot sector may overwrite part of the directory.

 Copyright © Dr Solomon's Software

Variants

There are a large number of variants, as it is easy to patch the message: **Zapper, Sanded, June 4th.a, Sex Revolution 1.1** and **2, Swedish Disaster, Rostov, Stoned-8, Stoned-16, Stoned.16.a, Damien, Bravo, Laodung, Noint (Bloomington), Azusa.a, Bunny.a, Daniela, Dinamo Empire.INT.10.b, Standard.a, Lzr, Empire.Monkey.a, Empire.Monkey.b, Kiev, NOP, Manitoba, W-Boot, Michelangelo.a,** and **No INT.a.** Other variants: **Teraz, b, c, d, e, Sonus, Nulls, Donald, Flushed, In love, stoned-floppy, Mexican,** and **WD1** to **WD7**.

Stoned dropper

Type

Dropper.

Affects

Floppy disks.

File Growth

-

Description

This is not a virus but a virus-dropper. It does not replicate. It purports to be a program which formats floppy disks, but it also installs a copy of ***Stoned*** on the boot sector of each disk. The example that was examined was called CFORMAT.COM.

Striker

Type

File virus.

Affects

COM files on execution of an infected file.

File Growth

461 bytes.

Description

The text **`Striker #1`** can be found near the start of the file.

Copyright © Dr Solomon's Software

STSV

Type

File virus.

Affects

All COM files in the current sub-directory of drive C (regardless of the current drive) on execution of an infected file.

File Growth

200 bytes.

Description

The virus contains the text **STSV**.

Stupid (Do nothing)

Type

File virus.

Affects

The first COM file in the current sub-directory when an infected file is run. Date/time and read/write attributes are not preserved.

File Growth

583 bytes.

Description

There is no self-recognition code, so files can be re-infected. Eventually, running an infected file will crash the system.

Suomi

Type

File virus.

Affects

A COM file on execution of an infected file.

 Copyright © Dr Solomon's Software

File Growth

1,008 to 1,023 bytes.

Description

When a file has been infected for 17 days, the virus disinfects that file, disables the keyboard, writes rubbish to the screen, and hangs the PC.

Superhacker (Murphy, Talentless Jerk, Harare)

Type

File virus.

Affects

COM and EXE files on execution of an infected file. Only files between 9 and 61,440 bytes are infected.

File Growth

1,077 bytes.

Description

The file contains **`Murphy`**, but the message is encrypted.

If the date is a multiple of 4 and the seconds are a multiple of 4, the virus displays **`Craig Murphy calls himself SUPERHACKER but hes just a talentless jerk!`**. It creates a file called `^^^^^^^^` in the root directory, then deletes it. EXE files are disinfected when they are run.

This is completely unrelated to ***Murphy-1*** and ***Murphy-2***.

SVC (SVC 5.0)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. Only files between 1,024 and 63,811 bytes are infected.

File Growth

Version 4: 1,689 bytes. This is concealed from DIR if the virus is in memory.

Copyright © Dr Solomon's Software

Description

The text `(c) 1990 by SVC,Vers 4.0` can be found at the end of the virus.

Variants

SVC 3.1:

Files grow by 1,064 bytes. COM files of less than 1Kb, or of 25,312 or 25,307 bytes, possibly to avoid infecting some versions of COMMAND.COM. It also avoids infecting programs with AI or SC in the name. This is probably to avoid infecting AIDSOUT (a Russian anti-virus program) and SCAN. The virus contains the text `(c) 1990 by SVC,Vers. 3.1`.

SVC 5.0:

Files grow by 3,103 bytes. The virus is fully stealthed.

SVC 6.0:

Files grow by 4,644 bytes. The virus is fully stealthed. It also infects partition sectors.

SVC.3103.a.

SVIR

Type

File virus.

Affects

The next EXE file in the current sub-directory on execution of an infected file. Attributes and date/time are not preserved.

File Growth

512 to 527 bytes.

Description

After using the file for a while there will be a large number of unrequested accesses to drive A.

The virus contains a counter which starts at 55, and each time an infected program is run the counter is decremented. When the counter reaches zero, it tries to access drive A each time the infected program is run. If there is no disk in the drive the normal error message will be displayed.

 Copyright © Dr Solomon's Software

Swami (Bhaktivedanta)

Type

Memory resident file virus.

Affects

COM and EXE files on execution, except those matching *ND.COM (so COMMAND.COM is not infected). COM files between 1,250 and 64,000 bytes and EXE files between 1,250 bytes and 64Kb are infected.

File Growth

1,250 bytes.

Description

The text string **`Bhaktivedanta Swami Prabhupada (1896-1877)`** can be found in the virus. If a file matching the name *AN.EXE, *LD.EXE or *RJ.EXE is run, the virus attempts to re-boot the PC with an interrupt 19h. On some machines this re-boots but on others it hangs the system. On Saturdays, if a COM file is run the first EXE file in the directory is deleted. Every April 15th, an EXE file is deleted each time a program is run.

The virus uses part of the *Dark Avenger* code to access the firmware for writing to the disk instead of going via interrupt 13h.

Swiss-143 (Zany.143a)

Type

Non Resident file virus.

Affects

COM files on execution of an infected file.

File Growth

143 bytes.

Description

This virus puts its code at the beginning of the infected file. Original file contents (exactly 143 bytes) are moved to the end of the file.

Copyright © Dr Solomon's Software

Swiss Boot (Swiss, Swiss Army, Armee)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The virus uses 3Kb of RAM (6Kb when the PC is booted from an infected floppy disk, since the virus does not check for itself in memory). It does not use stealth.

The virus occupies three sectors on disk; the infected boot sector and two other sectors, contain the main body of the virus.

On an infected floppy disk, the original boot sector and two sectors of virus code are stored on the first 3 clusters of the floppy disk. These sectors are marked as bad in the FAT, which is reported by CHKDSK as '2 lost allocation units found in 2 chains.

On the 2nd, 7th and 11th of February (variants **a**, **c** and **b**, respectively) these viruses display a message and overwrite the hard disk. The messages for variants **a** and **b** are:

```
Schaft die Schweizer Armee ab!

Auslander raus aus der Schweiz!"
```

Variants

a-c.

Sylvia (Holland Girl, Holland)

Type

File virus.

Affects

Four uninfected COM files on execution of an infected program. IBMBIO.COM, IBMDOS.COM and COMMAND.COM are avoided, presumably to avoid detection.

 Copyright © Dr Solomon's Software

Attributes are preserved. This is one of the few viruses that infects by making an infected copy and deleting the original.

File Growth

1,332 bytes.

Description

When an infected file is run there is a lot of disk activity as the virus looks for a file to infect.

The message **`This program is infected by a HARMLESS text-Virus V2.1 Send a FUNNY postcard to : Sylvia Verkade, 1 Duinzoom 36b, 3235 CD Rockanje The Netherlands. You might get an ANTIVIRUS program.....`** is in the virus but is not displayed.

The virus checksums this message each time it runs, and if it has been altered it displays:

```
FUCK YOU LAMER!!!!

system halted...
```

and the system hangs.

Variants

Kranz:

The text at the beginning has been altered to **`This program is infected by a ******** KranzVirus *12*`** and the address has been changed. Because the checksum has not been patched, the PC hangs when it is run. The message which should be displayed has been patched using asterisks. Since running this virus hangs the PC, it cannot spread.

Hong Kong:

This does not work. It contains a political message.

Minor variants: **a**, **b**, **c**, and **d**.

Syslock (Macho, 3551, Macrosoft)

Type

File virus.

Copyright © Dr Solomon's Software

Affects

A COM or EXE file (chosen randomly from the current drive) on execution of an infected file. The virus is encrypted and decrypts itself at run time. The virus looks for a DOS sub-directory off the root, and if it finds one creates a hidden system file called KEYB.PCM.

File Growth

3,551 to 3,566 bytes.

Description

If the environment contains SYSLOCK=@ the virus does nothing – it does not even infect files. Otherwise, it works its way down the disk, 32 sectors at a time, converting each occurrence of the word Microsoft to Macrosoft (or Machosoft in the *Macho* version). It uses KEYB.PCM to mark the point it has reached in making the changes. If there is no sub-directory off the root called DOS, it does not create the KEYB.PCM file and so does not make the changes.

Variants

Cookie (Cookie-2232):

Files grow by padding to a multiple of 16 bytes then adding 2,232 bytes. If the year is 1988 or later and the date is April 1st or later, running an infected program sometimes triggers the trick. The screen clears and **`I want a Cookie!`** is displayed in the centre. If you type **`Cookie`** the original program will run.

Xmas:

This is a variant that displays a growing number of candles on the days up to Christmas.

Tai-Pan.434

Type

Memory resident file virus.

Affects

EXE files on execution. The virus uses 496 bytes of memory.

File Growth

434 bytes.

 Copyright © Dr Solomon's Software

Description

The virus is an unencrypted, appending EXE file infector, containing the following strings:

`whisper presenterar Tai-Pan` and **`CoSmO`**.

Self-recognition in memory is INT_21 with AX=7BCE. The correct response is AX=7BCE.

The virus uses the perfectly legal INT 21/AH=48 function to go memory resident.

The virus garbles all file-writes except its own and is very noticeable.

Tai-Pan.438

Type

Memory resident file virus.

Affects

EXE files on execution. The virus takes 496 bytes of memory.

File Growth

438 bytes.

Description

The virus is an unencrypted, appending file infector, containing the following string:

`Whisper presenterar Tai-Pan`.

Self-recognition in memory is INT_21 with AX=7BCE. The correct response is AX=7BCE.

The virus uses the perfectly legal INT 21/AH=48 function to go memory resident.

Variants

a, **b**.

Variants **a** and **b** differ only in the first 39 bytes which are zero in *Tai-Pan.438b* (in fact, variant **b** is a damaged, but still working variant **a**.

Tai-Pan.666 (D2D, Doom2Death, Doom II Death)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

EXE files (MZ signature) on execution. It does not infect files of less than 64,768 bytes.

File Growth

-

Description

The virus contains the following string:

```
Your version of DOOM2.EXE matches the illegal RAZOR release of
DOOM 2 Say bye-bye HD The programmer of DOOM II DEATH is in no
way affiliated with ID software. ID software is in no way
affiliated with DOOM II DEATH.
```

Taiwan-708

Type

File virus.

Affects

An uninfected COM file on execution of an infected file. The DOS write-protect error message is suppressed. Date/time and read/write attributes are preserved except that the seconds field is set to 62.

File Growth

708 bytes, or to 1,416 bytes if they are less than 708 bytes.

Description

Program loading is slowed by the search for uninfected files.

On the 8th of any month, garbage is written to the first 320 sectors of the current drive and drive D, starting at the boot sector and overwriting both FAT copies and the root directory. The message **`Greetings from the National Central University! Is today sunny?`** is then displayed.

Variants

Taiwan-743:

Files grow by 743 bytes, or by 1,486 bytes if they are less than 743 bytes. Only 160 sectors are over-written, and after the message it waits for a keypress.

 Copyright © Dr Solomon's Software

Tchechen

Type

Memory resident, file virus.

Affects

COM and EXE files upon execution.

File Growth

-

Description

Variants: 1909, 1919, 3430, 3470, 3560

All variants (except the **1909** variant) trojanize the partition sector by putting code which will print on 22nd -25th of every month:

```
HALF YEAR OF WAR HAS GONE.  IT STILL DOES.

MASS MURDER RECOGNIZED BY THE WORLD COMMUNITY.

ACCEPT MY CONGRATULTIONS!  ENJOY THE WORLD'S NEW ORDER!  THE
TCHECHEN, v 2.0 (C)

RUSSIAN BEAR.  1995, JUNE
```

Variant **3470** also contains the sub-string `'v.2.0 spec'`

Variants **1919**, **3430** and **3470** were deliberately programmed to complicate repair - all repair data is scattered all over the file and encrypted with different keys.

Variant **3560** contains anti-emulation code, in an attempt to make analysis and detection more difficult.

Telefonica (Kampana-boot, Campana)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Copyright © Dr Solomon's Software

Description

If the PC is booted from an infected floppy disk, the virus infects the partition sector of the hard disk. The virus then infects any floppy disk accessed while the virus is memory resident.

On hard disks, the virus copies the original partition sector to cylinder 0, head 0, sector 7. The virus also stores additional code in sectors 6 and 7. On floppy disks, the original boot sector is copied to one of the root directory sectors.

When the virus is memory resident, it uses stealth to conceal itself. If the partition sector is examined, the virus displays the original, clean partition sector, and if sectors 6 and 7 are examined, the virus displays sector 5.

After 400 boots from an infected hard disk, the trojan triggers, overwriting the hard disk with garbage and displaying the text:

```
Campana Anti-TELEFONICA (Barcelona)
```

which is encrypted in the virus.

Tenbytes (1554, Usenet, 1559,9800:0000, Valert)

Type

Memory resident file virus.

Affects

COM files (greater than 1,000 bytes) and EXE files (greater than 1,024 bytes) on execution. Read/write attributes are preserved.

File Growth

COM: 1,554 to 1,569 bytes.
EXE: 1,514 to 1,529 bytes.

Description

Between September and December, whenever DOS writes to a file, the first 10 bytes are omitted and 10 bytes of garbage are added at the end. Program and data files are infected.

The memory resident part of this virus is in memory that has not been reserved. This makes it vulnerable to being overwritten, but it will be undetectable by memory map programs.

 Copyright © Dr Solomon's Software

Tentacle

Type

File virus.

Affects

One file in the current directory, followed by two files in the Windows directory.

File Growth

1966 bytes.

Description

A sample of the virus was found on the alt.cracks newsgroup, attached to a posted file called DOGZCODE.ZIP.

The virus only infects NE-EXE files (this is a format of Windows 3.0+ 16-bit applications: such applications are compatible with Windows 95 and Windows NT)

The payload acts between midnight and 12.15a.m. A program that becomes infected within this time has its standard icon changed to an icon of a tentacle. This change is not immediately obvious. It is not until you attempt to change the icon, delete the icons in the program group and attempt to replace them, or if you run and minimize the program, that the tentacle icon will display itself.

Tequila

Type

Multipartite virus.

Affects

When an infected EXE file is run, the virus installs itself on the partition sector and on five sectors at the end of the partition (*Tequila* patches the partition data to reduce the length of the partition by six sectors). When the PC is next booted, the virus goes memory resident and infects EXE files (except those with a V or SC in the name, thus avoiding anti-virus programs like VIR or SCAN, which are often self-checking).

File Growth

2,468 bytes.

Description

Tequila is polymorphic and uses stealth to conceal itself when memory resident.

Copyright © Dr Solomon's Software

If the partition sector is examined, the virus displays the original, clean partition sector. However, it does not stealth the five sectors at the end of the partition sector (including the original, clean partition sector).

If an infected program is run three months after the partition sector became infected, the virus displays a large colored graphic and, at the top of the screen, the text:

```
Execute: mov ax, FE03 / int 21. Key to go on.
```

If these instructions are executed, the following message text is displayed:

```
Welcome to T.TEQUILA's latest production. Contact T.TEQUILA/
P.o.Box 543/6312

St'hausen/Switzerland.

Loving thoughts to L.I.N.D.A

BEER AND TEQUILA FOREVER !
```

This text can be found in one of the sectors at the end of the partition.

Variants

2468.a-c, 2469.

Terror

Type

Memory resident file virus.

Affects

COM and EXE files on execution or opening. COM files must be between 1Kb and 64,000 bytes.

File Growth

1,085 to 1,100 bytes.

Description

The virus contains `Terror` at the end.

Testvirus B V1.4

Type

File virus.

 Copyright © Dr Solomon's Software

Affects

All COM files in the current sub-directory on execution of an infected file, but only if you choose the 'infect' option (see the Description below).

File Growth

1,000 bytes.

Description

Files contain **`This is TESTVIRUS B V1.4`** near the beginning. This is displayed each time the program runs. Then it gives the options:

```
1 = infect .COM files of this directory
    and run the original program

5 = run only original program

9 = abort
```

Thanksgiving (V1253)

Type

Multipartite virus.

Affects

COM files on execution. The partition sector is infected when an infected COM file is run, or if the PC is booted from an infected floppy disk. Any floppy disk accessed when the virus is memory resident is infected. Date/time and read/write attributes are not preserved.

File Growth

1,253 bytes.

Description

Floppy disks: The original, clean boot sector is moved further up the disk.

Hard disks: The original, clean partition sector is moved further up the disk.

When the virus is installed by booting from an infected disk, 64Kb of memory is no longer available.

On the 23rd November 1990, and thereafter, the payload is triggered. This overwrites 17 sectors on heads 0 and 1 of the hard disk, stepping through the cylinders from 0.

Copyright © Dr Solomon's Software

There is no stopping point, so the virus will go as far as cylinder 255, then cycle back to 0 and continue. The hard disk will then be unreadable.

If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

22nd November 1990 is Thanksgiving Day in the USA.

The Rat

Type

Memory resident file virus.

Affects

EXE files on execution or opening.

File Growth

None. Overwrites 384 bytes of the header, starting at offset 128.

Description

The virus contains **`The Rat, Sofia`** at the end. There is also a message in Bulgarian inside, which is not displayed.

There is no payload.

Thirteen minutes (V711)

Type

Memory resident file virus.

Affects

COM files on execution. Only files greater than 1,700 bytes are infected. COMMAND.COM is avoided.

File Growth

704 bytes plus a random number in the range 0 to 15.

Description

Thirteen minutes after infection there is a 25% chance of each disk failing to write and giving a time-out error code.

 Copyright © Dr Solomon's Software

Three_Tunes.1784 (3tunes, JuneTunes, Pichincha, PC Byte Bandit)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

Description

This virus was first reported in a small province Pichincha in Ecuador.

Three_Tunes.1784 is encrypted. It uses stealth to conceal itself when memory resident. It is also a fast infector, intercepting Open (3d) and Execute (4B00) DOS functions.

The virus intercepts INT_01 (trace), INT_1Ch (timer), INT_21h (DOS services), INT_24h (critical errors). The virus checks for itself in memory by issuing a call, AX=FE01/INT_21h; the correct response is AX=01FE.

To recognize files which it has infected already, the virus checks two bytes at offset eof-69 (-45h); all infected files contain 0E 1F at this location.

The virus does not check the extension of the opened file and assumes all files which start with an E9 byte to be COM files suitable for infection. As a result, the virus can corrupt data files. It will also corrupt NE executable files; and DLLs, because it regards all files starting with "MZ" as being EXE files.

The payload activates in June. Any infected program will either play one of three built-in melodies or just execute the host file. Music is played with the probability 75%.

Thursday-12th

Type

Memory resident file virus.

Affects

COM and EXE files on execution, opening or creation. COMMAND.COM and any files starting with SCAN, CLEAN, VIR, ARJ and FLU are avoided.

Copyright © Dr Solomon's Software

File Growth

2,161 to 2,176 bytes.

Description

The virus contains the encrypted text **`VirCheck V1.2 (C)1991 Be aware of those worms out there, violating your machine on Friday 13th - it's tomorrow!`**, but this is not displayed.

Tiny

Type

Memory resident file virus.

Affects

The first uninfected COM file in the current sub-directory on execution of an infected file.

File Growth

Varies depending on the variant: 133, 134, 138, 143, 154, 156, 158, 159, 160, 167, or 198 bytes.

Description

There is no payload.

Variants

Eleven, with sizes as listed in File Growth.

Tiny-127

Type

File virus.

Affects

A COM file in the current sub-directory on execution of an infected file. Date/time is not preserved.

File Growth

127 bytes.

Copyright © Dr Solomon's Software

Description

There is no payload.

Tiny-128

Type

Memory resident file virus.

Affects

COM file on execution.

File Growth

128 bytes.

Description

The virus overwrites the upper end of the interrupt vector table. Date/time is not preserved. There is no payload.

Tornado

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

This virus infects the boot sector of floppy disks and the partition sector of hard disks. It uses stealth to conceal itself when memory resident and is encrypted with a variable encryption key.

The original partition sector is moved to cylinder 0, head 0, sector 14.

On floppy disks, the original boot sector is moved to:

5.25", 360Kb disks: cylinder 0, head 1, sector 3

5.25", 1.2Mb disks: cylinder 0, head 1, sector 14

Copyright © Dr Solomon's Software

3.5", 720Kb disks: cylinder 0, head 1, sector 5

3.5", 1.44Mb disks: cylinder 0, head 1, sector 14

Tornado causes 1Kb to be missing from DOS memory. On most machines CHKDSK will report **`654336 total bytes memory`** while normally it is 655360.

Under certain conditions, *Tornado* can shift the screen display continuously from right to left. This screen shift is halted by pressing the Esc key.

The virus contains the encrypted text **`TORNADO`** which is not displayed.

Traceback (3066)

Type

Memory resident file virus / file virus.

Affects

There are two mechanisms:

Memory resident, infecting COM and EXE files on execution;

Direct action (after December 1988), infecting a COM or EXE file on execution of an infected program.

The resident portion of the virus occupies 7Kb of memory.

File Growth

3,029 to 3,066 bytes.

Description

An hour after the virus goes memory resident a falling letters display is triggered. This is different from *Cascade* in that the display is silent and the characters fall in a different way. They can be made to rise up again by pressing keys until they are all at the top of the screen. This is purely cosmetic and there is no damage done to data.

Variants

Spanish (Traceback-2930):

An earlier version. Files grow by 2,930 bytes.

 Copyright © Dr Solomon's Software

Track Swap (Trkswap, XBoot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks.

File Growth

-

Description

This virus uses 1Kb of RAM and occupies one sector on the disk. The virus swaps the 9 first sectors (both heads 0 and 1) on cylinders 0 and 39 of floppy disks, which is how it gets its name.

Track Swap intercepts INT_13h (disk I/O) and INT_09 (keyboard). When [Ctrl]-[Alt]-[Del] is pressed the virus infects the floppy disk in drive A: if there is a disk in the drive. For self recognition, the virus uses bytes 33 FF at the very start of the infected sector.

Trakia (Ugur, Corgi, TEKRAR)

Type

Memory resident file virus.

Affects

COM and EXE files (but see Description below).

File Growth

See Variants.

Description

Variants **561** and **570** infect COM and EXE files; variant **661** infects EXE files only. Variant **1070** infects COM and EXE files when they are run, but also infects all EXE files in the current directory when programs are run.

Only interrupt 21h is intercepted. The **561** and **570** variants check for themselves in memory by issuing a call, AX=4343/INT_21h; the correct response is AX=3434. Variant **661** uses FE43 -> 3434. Variant **1070** uses 4288 -> 4288.

Copyright © Dr Solomon's Software

This virus has no payload.

Variants

561, 570, 661, 1070.

Variant **570** blanks the date and time of all files it infects.

Trash

Type

-

Affects

-

File Growth

-

Description

The program displays the message:

```
********** W A R N I N G ! ! ! **********

This program, when run, will zero (DESTROY!) The master boot
record of your first hard disk.
```

Then it explains that its purpose is to test anti-virus software. You have to press Ctrl Alt to proceed, a combination which would be very hard to press accidentally.

This demonstrates that a hard disk can be trashed even though a protection program is installed. It does so successfully.

Tremor

Type

Memory resident file virus.

Affects

COM and EXE files on execution and almost any access. COM files are infected only if they start with 0E9h (a JMP instruction).

 Copyright © Dr Solomon's Software

File Growth

4,000 bytes.

Description

This virus is variably-encrypted and highly polymorphic.

When an infected file is executed, the virus goes memory resident, possibly in the Upper Memory Block or Extended Memory (if available), and infects COMMAND.COM. The virus uses full stealth to conceal itself when memory resident. This virus is a 'fast infector', which makes it essential for any scanner to detect it if it is active in memory.

Approximately three months after infecting the PC the virus triggers. On every Ctrl Alt Del warm boot the following message is displayed:

```
-= T.R.E.M.O.R. was done by NEUROBASHER
/May-June'92 Germany =-

-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-
```

In addition, if more than 255 files were created or opened (for example, via the COPY command) since the last system re-boot, the virus starts to salute every DOS call with a random sound and screen display tremor.

Variants

4000.a-c.

Trivial

Type

Overwriting file virus.

Affects

The first COM file in the current sub-directory.

File Growth

None.

Description

The virus is only 30 bytes long. Both program and data files are overwritten.

Copyright © Dr Solomon's Software

Variants

There are a number of versions and re-writes of this virus, with lengths between 25 and 200 bytes. All of them are overwriting viruses and cannot be a genuine threat.

Trojector (Athens)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

Trojector is an encrypted virus.

It checks for itself in memory by issuing a call: AH=BB/INT_21h; the correct response is AH=18.

The virus has no payload but the following strings (specific to each variant) are found in the virus:

```
1463: "TROJECTOR II,(c) Armagedon Utilities, Athens 1992"
1561: "TROJECTOR ]I[,(c) Armagedon Utilities, Athe"
```

Variants

1463, 1561.

Tumen

Type

Memory resident file virus.

Affects

A COM file on execution of an infected file. Files greater than 64,885 bytes are not infected. Date/time and attributes are not preserved.

File Growth

1,092 to 1,663 bytes, depending on the variant.

 Copyright © Dr Solomon's Software

Description

Tumen.1663 contains the text, **`Full moon tonight... The time of Wolfbacks... U...U...U... This is only demonstration version, but you hear some howl.`**

Near the end is the text:

`(C) Copyright MMA Company All rights reserved. USSR Tumen 1990-v0.5 This program was created in Tumen by group three Wolfbacks at April,1990 General System_&_Files affecting effects by Max Main consultant -Tall Lazy Micle General Music_&_Video harmless effects by Alex BACKWOLFS OF THE WORLD, UNITE ! ! !`

If you press Ctrl Alt and any key, a tune is triggered and screen palette effects are displayed on EGA and VGA monitors. Each time a file is infected the screen palette effect is triggered.

Variants

Tumen.1092:

This is very different but somewhat related. Files grow by 1,092 bytes and the virus contains the text **`Be carefull... Hackers time tonight... This present was created in Tumen at 1990. v.2.0.(c) Max Soft corporation`** and **`Hackers of the world, Unite !.`**

There is a counter (set at 51 in the specimen we have seen) which is incremented each time a file is infected. When the counter reaches 112 the trojan triggers, which overwrites cylinders 0 to 255, head 0, sectors 1 to 16. Before the trojan triggers, each time an infected file is run the virus reads the boot sector and writes it back unchanged. Presumably this is to acclimatize the user to any interrupt blocker giving regular false alarms.

While the virus is memory resident, files cannot be deleted or renamed. Possibly this is a defense against any anti-virus product which may attempt to remove the virus or rename infected files, while the virus is active in memory. Files of greater than 64,000 bytes are not infected.

Two other variants are **Tumen.1255** and **Tumen.1242**.

TUQ (RVPS)

Type

File virus.

Copyright © Dr Solomon's Software

Affects

A COM file on execution of an infected file.

File Growth

453 bytes.

Description

The virus contains the text **VIRUS**. It has no payload.

Twelve Tricks

Type

Trojan.

Affects

Leaves part of itself on every infected hard disk.

File Growth

-

Description

This is a program run by the user. As well as the obvious things, it lays down a new partition sector, containing the text **SOFTLoK V3.0 SOFTGUARD SYSTEMS INC 2840 St. Thomas Expwy, suite 201 Santa Clara, CA 95051 (408)970-9420.**

IMPORTANT: it should be pointed out that there is no evidence that the company mentioned has anything whatsoever to do with the trojan. Perhaps the author has a grudge against them.

When the partition sector is run,(every time the PC is booted from the hard disk), the trojan installs itself in memory. A random number generator determines which of the 12 tricks will be installed:

1. Insert a random delay loop in the timer tick. This slows down the PC, which runs jerkily.
2. Insert an End-Of-Interrupt in the timer tick. This interferes with the servicing of hardware interrupts so that, for example, the clock is stopped, or TSRs which depend on the timer tick do not work, or the floppy drive motor is permanently on.

Copyright © Dr Solomon's Software

3. Each time a key is pressed or released, the timer tick count increments by a random number. This means that programs sometimes will not run, or when you type '**TIME**' you get **Current time is divide overflow,** or copying files sometimes doesn't work.
4. Each time interrupt 0Dh is executed, the routine is completed only three times out of four. This interrupt is used on PCs and XTs for the fixed disk, and on ATs for the parallel port.
5. Each time interrupt 0Eh is executed, the routine is completed only three times out of four. This interrupt is used for the floppy disk.
6. Each time interrupt 10h (the video routine) is called, a random delay loop is inserted. This slows down the screen and makes it run jerkily.
7. Each time the video scroll up routine is called, instead of scrolling the requested number of lines it blanks the entire scrolling window.
8. Each time a request is made to the floppy disk handler, it is converted to a write request. Thus the first time you try to read from, or write to, a disk, whatever happens to be in the buffer will be written to and will probably overwrite, the boot sector, FAT or directory, as these must be read before anything else can be done. If you try to read a write-protected disk, the DOS **write-protect error** message is displayed. If you do a DIR of a write-enabled disk the **General failure...** message is displayed. If the disk is inspected using a sector editor, the boot and FAT will have been zeroed or overwritten.
9. Each time interrupt 16h (read the keyboard) is called, the flags for **Caps Lock**, **Num Lock, Shift**, and so on are set, randomly before the keystroke is returned. This means that the keyboard will work only occasionally at the DOS prompt, and programs which poll interrupt 16h will be unusable. Holding down the Del key will trigger a warm re-boot.
10. Everything that goes to the printer is garbled by XORing it with a byte from the timer tick count, which is in effect a random number.
11. Each character sent to the printer has its case reversed by XORing it with 20h. Non-alpha characters are XORed so that a 'space' becomes a null and 'line feeds' do not feed lines.
12. Each time the Time-Of-Day interrupt is executed, an End-Of-Interrupt is executed instead. This means that the system clock cannot be set and the time is set permanently to one value.

Copyright © Dr Solomon's Software

There are two more things the trojan does. It uses a random number generator to trigger a low-level format of the cylinder containing the active boot sector, one time in 4,096, which will also destroy part of the first copy of the FAT. Then it displays the message from the modified partition sector and hangs the PC. If it does not do the format, it makes a random change to a random word in one of the first 16 sectors of the FAT, which will cause a slight, increasing corruption in the file system. This is perhaps the worst thing it does, as it will cause an increasing corruption of the files on the disk.

The program that drops the trojan was, in the analyzed specimen, a hacked version of CORETEST, which is a program to benchmark hard disk performance. Although this is not a virus, it is unlikely that all the patching to the original program was done by hand. It is far more likely that the author wrote a prepender program to automatically attach his code to the target executable file. If this is the case, there are two consequences: a) other programs might have been trojanized (in other words, there may well be other droppers around), b) the encryption cannot be relied upon to have the same seed each time, as the prepender could change the seed each time it operates. So it would be unsafe to search files for the encrypted partition sector.

Indeed, a further possibility exists, in that the prepender program might have been placed into circulation and people running it could unwittingly be creating additional droppers. There is absolutely no evidence to suggest that this is actually the case, but anyone who detects this dropper in one of their files should take great care to examine all the others.

Twin

Type

Companion virus.

Affects

Each time an EXE file is run, a hidden COM file is created with the same name. When the program name is typed, the COM file is run instead of the EXE file, making the virus memory resident. Then the virus runs the EXE file.

File Growth

None.

Description

If the virus is in memory, DOS does not report the hidden files.

 Copyright © Dr Solomon's Software

Unashamed

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Unashamed uses 1Kb of RAM. On infected hard disks the original partition sector is re-located to cylinder 0, head 0, sector 14. The location of the original boot sector on floppy disks depends on the geometry of the floppy disk: cylinder 0, head 1, sectors 3, 5 or 14 (one of the last sectors of the root directory).

For self recognition of infected disks, the virus uses bytes 05 1A at offset 1BBh in the infected partition or boot sector.

The virus checks the system timer and sometimes turns the monitor into 40 column mode and prints the following message in the upper left corner:

```
the UNashamed Naked!
```

Urkel

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

Urkel uses 2Kb of RAM and occupies just one sector. Infected sectors always start with EB 22 90. On hard disks, the original partition sector is re-located to cylinder 0, head 0, sector 5. On 1.44Mb floppy disks, the original boot sector is re-located to the

Copyright © Dr Solomon's Software

very end of the root directory, cylinder 0, head 1, sector 15 (sector 3, 5 or 14 on other floppy disks).

The virus is encrypted. When the virus gets control it moves itself to

segment 9F80, decrypting the body on the fly (the virus assumes that all PCs have 640k of RAM because segment 9F80 is just 2Kb below the 640Kb limit).

For self recognition ***Urkel*** uses byte 23 at offset 1FDh in the infected partition or boot sector.

It displays the string **`Urkel`** if the disk is being written to and the current hour is 0 (12pm). This string is visible only in memory, at 9F80:1F7.

Uruguay.6 (Uruguvau)

Type

Memory resident file virus.

Affects

COM and EXE files on execution, opening or creation of an infected file. Files of less than 57,344 bytes are not infected. COMMAND.COM and some anti-virus programs are avoided.

File Growth

4,879 bytes.

Description

This variably encrypted and extremely polymorphic virus is able to survive a warm PC-boot (Ctrl Alt Del). It is a semi-stealth virus, that is, the growth of infected files is concealed when the virus is memory resident.

If an infected file is executed when the virus is already memory resident, there is a probability of 1-in-256 that the virus will trigger and display this message followed by a random tune:

```
'Uruguay-#6' Virus
programmed in Montevideo (URUGUAY) by F3161.11/92
This is a research virus - DO NOT DISTRIBUTE.
```

The virus can also trigger on a warm re-boot.

 Copyright © Dr Solomon's Software

Variants

Uruguay.1 to **Uruguay.8**. They differ in their levels of polymorphism, infected file growth and displayed messages. Earlier versions are less polymorphic and cannot survive a warm re-boot.

USSR-707 (V707)

Type

Memory resident file virus.

Affects

COM files on execution. Only files of less than 61,440 bytes are infected. This works only on DOS 3.3 systems.

File Growth

707 bytes.

Description

There is no payload.

V2P6

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

1,900 to 2,400 bytes.

Description

This virus is so polymorphic that there is not even a consistent sequence of two bytes for signature scanners to identify.

This is in the same family as *Chameleon*.

Copyright © Dr Solomon's Software

V-Sign (Cansu, Sigalit)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

The partition sector becomes infected when the PC is booted from an infected floppy disk. The virus then infects any floppy disks accessed with the virus memory resident.

V-Sign is slightly polymorphic. It changes the order of some instructions on every infection, resulting in six slightly different 'incarnations'.

The virus can detect disks infected with ***Stoned***, which it removes and then re-infects the disk with itself.

If the virus succeeds in infecting 64 disks since the last system boot, it triggers. A big V-sign is displayed on the screen and the PC hangs.

Vacsina.TP-05 (RCE-1206)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

Description

-

Variants

a.

 Copyright © Dr Solomon's Software

Vacsina.TP-16 (RCE-1339)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

-

Description

-

Variants

a.

Vbasic

Type

File virus.

Affects

Four COM or EXE files (starting in the current directory) on execution of an infected file. EXE files are infected before COM files. BASRUN.EXE, BRUN.EXE, IBMBIO.COM. IBMDOS.COM and COMMAND.COM are ignored. Date/time and read/write attributes are preserved.

File Growth

5,120 to 5,135 bytes.

Description

COM files are not infected correctly and infected COM files don't work. When an infected file is run there is a lot of disk activity as the virus looks for files to infect.

After April 1st 1992, when an infected program is run it infects all other programs on the disk and displays the **`Access denied`** message on the screen.

This virus looks as if it has been written in a higher level language than assembler, due to the way each sub-routine is called.

Copyright © Dr Solomon's Software

Variants

Vbasic.B:

File growth is 5,120 bytes, but the filenames used are different: KEYB*.COM, KEYB*.EXE, BRUN, BASRUN, COBRUN, and NET$OS.

Vbasic.C:

As **Vbasic.B**, but the filenames used are BRUN, BASRUN, COBRUN, NET$OS, LOGIN, USERLIB, and AV.

Vcomm (Polish, 637, Vcomm.A)

Type

Memory resident file virus.

Affects

An uninfected EXE file in the current sub-directory on execution of an infected file. During infection files are renamed with no extension. If the system hangs in the middle of the infection process the user is not left with a partly infected file. Read/write attributes are preserved. If the virus tries to infect a write-protected disk the DOS message **`Write protect error writing drive X: Abort, Retry, Ignore?`** is given.

File Growth

637 to 1,148 bytes.

Description

The virus installs a small routine which converts all disk-writes to reads. Thus, as long as it is in memory, the user cannot create, copy, change or delete a file. On monochrome systems the first disk access will hang the system. CGA monitors show a slight snow effect.

VDV-853

Type

File virus.

Affects

A COM file on execution of an infected file.

Copyright © Dr Solomon's Software

File Growth

853 bytes.

Description

The messages are encrypted in the virus so they can't be seen.

Between December 24th and 26th, when an infected file is run, it displays a Christmas tree in block graphics with the message:

```
Frohliche Weihnacten wunscht der Verband Deuscher
Virenliebhaber Ach ja, und dan Daten von der Festpla
gez. VDV, December 1990
```

The next time a key is pressed, rubbish is displayed on the screen and COMMAND.COM is overwritten with the Christmas tree and message.

VFSI

Type

File virus.

Affects

A COM file in the same directory on execution of an infected file. Read-only files are ignored.

File Growth

445 to 453 bytes.

Description

Each time an infected program is run there is a 20% chance of the following: the display changes to 40-character mode, clears, and the message **`HELLO!!! HAPPY DAY and SUCCESS`** is shown in yellow, with **`from virus 1.1 VFSI-Svistov`** under it, shown blinking in red. Then the screen is cleared and the infected program runs normally.

Victor

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

A COM or EXE file on one of several DOS function calls. Files of less than 2,442 bytes and COM files of greater than 62,198 bytes are not infected. Date/time and read/write attributes are preserved.

File Growth

2,443 to 2,458 bytes.

Description

The virus contains the text **`Victor V1.0 The Incredible high Performance Virus Enhanced versions available soon. This program was imported from USSR. Thanks to Ivan.`**

On Wednesdays between 9 a.m. and 10 a.m., 11 a.m. and 12 noon, 1 p.m. and 2 p.m., and 3 p.m. and 4 p.m., files in the current sub-directory are deleted.

Vienna (648, 1-in-8, Austrian, DOS-62, First Austrian, DOS-68, Unesco, Charlie, Vienna-648, DOS-62)

Type

File virus.

Affects

The next uninfected COM file, in the current directory or accessed via the PATH, on execution of an infected file in any directory.

File Growth

648 bytes.

Description

One-in-eight infections make the file unusable by patching code for a re-boot at the beginning of the file. Eventually COMMAND.COM is infected, so that whenever the PC is started up it just keeps re-booting. The seconds field of the directory is used to store the impossible value 62, as a self-recognition.

Variants

The source code for this virus has been published in a book, with slight modifications, so there are a large number of viruses based on it. It is commonest in Austria, where it has been given several names. The patching code in the typed-in

Copyright © Dr Solomon's Software

variants hang the machine, and they do not search down the path for an uninfected file.

The variants are all nearly functionally identical to the original, but there seems to have been attempts to reduce the byte-count. The name refers to the byte count/file growth.

The variants are: **Vienna-71a1, 822, Vienna-744 (Grither), 733, 716, 656, 648, 648.reboot.a, 646, 646b, 645, 644, 627, 623, 622, 583, 582, 535, 528, 510, 435, 367, 353,** and **348.**

Other variants have the sizes 361, 377, 534, 547, 618, 625, 634, 757, 774, and 776 bytes.

Vienna-534 (W13.A)

Type

File virus.

Affects

The next uninfected COM file in the current directory, on execution of an infected file.

File Growth

534 bytes.

Description

There is no payload, but infected files are dated the 13th of the month.

This is a modification of *Vienna.*

Variants

Vienna.W13B:

Files grow by 507 bytes.

Vienna-Iraqui

Type

File virus.

Affects

A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are infected.

Copyright © Dr Solomon's Software

File Growth

777 bytes.

Description

An error in the code means this cannot replicate more than once from the original file.

The virus contains the strings **`I come to you from The Ayatollah! (c)1990, VirusMasters`**

and

`An Iraqui Warrior is in your PC....`

One file in eight has a re-boot patched into the start of the file instead of being infected (except that the re-boot does not work). When this happens the second message is displayed.

This virus is very like *Vienna*.

Vinchuca.925

Type

Memory resident file virus.

Affects

COM files.

File Growth

925 bytes.

Description

This is an encrypted virus which infects COM files being run. It uses a prepending infection method.

It intercepts only INT 21h. To check for itself in memory the virus issues a call, AX=35E3/INT_21h; the correct response is BX=3775.

The payload activates when an infected file is run on the 3rd of any month. The virus displays the following message box:

```
Virus ViNCHuCa  V1.0  1993.
Creado por MURDOCK.
```


Copyright © Dr Solomon's Software

```
Buenos Aires ,Argentina.

Su PC tiene Mal de Chagas....jajaja...
```

On 3rd of July, it additionally overwrites the contents of the first hard disk (cylinders 0 to 256, heads 0 to 3, 17 sectors) and hangs. The string inside the virus reads:

```
Saludos para SaTaNiC BRaiN y Patoruzu
```

Variants

925.

Violator

Type

File virus.

Affects

A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are infected.

File Growth

1,055 bytes.

Description

The virus contains the text:

```
TransMogrifed (TM) 1990 by
RABID Ntnl Development Corp.
!!!!!!!!!!!!!!!!!!!!!!!!!!
!Copyright (C) 1990 RABID !
!Activation Date: 08/15/90!
!! - Violator Strain 1 !
!(Field Demo Test VErsion)!
! *NOT TO BE DISTRIBUTED* !
!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The payload is triggered on or after August 15th 1990. This does a low-level format of cylinder 0, head 0. The device to be formatted is randomly selected, but the virus then steps through all other devices.

This virus is another version of *Vienna*.

Variants

Violator B3:

Files grow by 843 bytes. After December 25th 1990 the virus tries to format drives C to Z, but fails. It also tries to overwrite the first 800 sectors of drive C with the text **`Violator Strain B3 - Rabid Nat'nl Development Corp..`**

Violator-Arf

Type

File virus.

Affects

A COM file on execution of an infected file. Only files between 10 and 64,000 bytes are infected.

File Growth

1,000 bytes.

Description

The virus contains the text **`Arf Arf Got You! - RABID 90.`**

If the date is after October 10th 1990 the message is displayed and physical drives 0 to 25 are formatted. Normally this means that the A and B drives are formatted.

This virus is very like *Vienna*.

Variants

Violator-arf.s:

If the year is 1992 or later, the virus displays **`If this one escapes, I am fucked up.`** When an infected program is run, it triggers the payload, which formats cylinder 0 head 0 of all floppy drives. It looks as though it was meant to format floppy and hard disks, but it contains a bug.

 Copyright © Dr Solomon's Software

Violator B4

Type

File virus.

Affects

COM files on execution of an infected file. Only files between 10 and 64,000 bytes are infected.

File Growth

5,302 bytes.

Description

The virus contains the string **`Violator Strain B4 - Written by The RABID Natn'l Development Corp.`** and several more lines of text. All interrupt 21h, 13h and 26h calls are done by calling sub-routines. This avoids the usual sequence of interrupts seen in most viruses.

The intention is to low-level format and overwrite all drives with garbage. This does not work because of bugs.

This virus is very like *Vienna*.

Virdem

Type

File virus.

Affects

The next uninfected COM file on drive A on execution of an infected file.

File Growth

Files of less than 11Kb grow by 2,559 bytes.

Files of greater than 11Kb grow by between 792 and 1,616 bytes.

Description

When an infected program is run, the user is asked (in German) to guess a number between 0 and n, where n is the generation number of the virus plus 1. If the guess is correct, the program runs. If the guess is wrong, control returns to DOS.

Copyright © Dr Solomon's Software

If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

This was written as a demonstration virus by Ralf Burger, and was distributed as such.

Variants

Virdem English:

The messages are in English instead of German.

Virdem Disktrash:

This trashes the hard disk if the guess is incorrect.

Virdem.2:

Files grow by 824 bytes. If contains the string **`Datum falsch Bitte DATE aufrufen`**. If the date is 1980 it displays the message and exits without running the host program.

Virdem-1542:

This is a partially-overwriting virus, but most programs will continue to work after infection. Files grow by 1,542 bytes (or more if the file is less than 1,542 bytes). The messages are patched out. There is no payload apart from some programs not working, as the infection overwrites four of the original bytes.

FindVirus should not be used to remove this virus. Infected files should be deleted and replaced with good copies.

Other variants are: **Wonderful** and **792**.

Virus-101

Type

File virus.

Affects

The next COM file on drive A or B on execution of an infected file. Date/time and read/write attributes are preserved.

File Growth

2,560 bytes.

Copyright © Dr Solomon's Software

Description

When an infected file is run on the 9th, 18th or 27th of the month a screen display is triggered (see below). This consists of white bars moving down the screen from the top. The PC is re-booted. On any other date the hard disk boot sector is patched. If the letters 'No' (as in **Non-system disk**) appear in the boot sector, everything from there on is replaced by:

```
This file has been safely infected by

VIRUS101 - the safe, educational virus utility.

This copy furnished to John McAfee.
```

This message is checksummed and if it is incorrect the program halts. If not, the message is displayed.

Variants

Virus-90:

An earlier version. Files grow by 857 bytes. When an infected program is run it displays **`infected!`** before running the program. The virus contains the name and address of the author.

Both these viruses were written as demonstrations so that people could safely experiment with them – hence the fact that they only infect drives A and B.

Virus-B (Friday 13th, 423)

Type

File virus.

Affects

All uninfected COM files in the current directory on execution of an infected file in any directory. COMMAND.COM is not infected. Date/time and read/write attributes are not preserved. If the virus tries to infect a write-protected disk the DOS **`Abort, Retry, Ignore?`** message is displayed.

File Growth

540 to 560 bytes, according to the version.

Description

Every Friday 13th, infected files are deleted after they are loaded into memory and executed. This does not prevent further infection.

Copyright © Dr Solomon's Software

Version 1:

When an infected file is run the PC beeps and the following message is displayed:

```
WARNING!!!! THIS PROGRAM IS INFECTED WITH VIRUS-B!
IT WILL INFECT EVERY ..COM FILE IN THE CURRENT sub-directory!
```

Version 2:

COM files grow by 423 bytes, but are not infected.

Virus Construction Set (VCS)

Type

File virus.

Affects

A COM file on execution of an infected file. The virus is encrypted, and if interrupt 26h is located above segment 1000h (for example, if an active monitor is enabled) it does not infect.

File Growth

1,077 bytes.

Description

This is a virus creation program enabling anyone to create viruses. However, the viruses it produces will always have a lot in common.

After n generations (where n is set at creation) it displays the message '`512 bytes set at creation`.'.

Voronezh

Type

Memory resident file virus.

Affects

COM and EXE files on opening. COMMAND.COM and COM files greater than 61,000 bytes are avoided.

File Growth

1,600 bytes.

Copyright © Dr Solomon's Software

Description

The virus contains the text **`Voronezh,1990 2.01`**. It has no payload.

Voronezh-600

Type

Memory resident file virus.

Affects

COM files on execution. Only files between 600 and 60,000 bytes are infected. Read-only files are not infected.

File Growth

600 bytes.

Description

There is no payload.

VP

Type

File virus.

Affects

A COM file (selected from any sub-directory on any drive except B) on execution of an infected file. Only files between 16 bytes and 63Kb are infected. Date/time is preserved. If the virus tries to infect a write-protected disk the DOS **`Abort, Retry, Ignore?`** message is displayed.

File Growth

Variable, calculated by rounding the size up to a multiple of 16 bytes and adding 909 bytes.

Description

After infection the virus looks at the system time. If the time is in the first five seconds of a minute, the screen is cleared and a message is written to the centre (this was zeroed out in the specimen that we received). Then the virus waits for a keystroke, clears the screen and exits.

Copyright © Dr Solomon's Software

Vriest

Type

Memory resident file virus.

Affects

COM files on creation, for example, when copied.

File Growth

1,280 bytes.

Description

On any day after May 3rd 1991, when a program terminates or goes memory resident the virus displays **`Something's coming up...`** and makes a descending sound. Then it displays **`Vriest of g greets Vic ear Moeli-.`**

Walker.3846 (Sleep_Walker)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

3845 bytes.

Description

The virus infects COM and EXE files on execution. It is not encrypted. This virus is able to remove itself from infected files.

The virus intercepts INT_16h (keyboard) and INT_21h (DOS services). It checks for itself in memory by issuing a call, AX=4B56/INT_21h; the correct response is AX=5641.

The payload displays a man walking from the right to the left of the screen. The picture of the man is formed from coloured pseudographic symbols. The virus is clearly demonstrative. Most of the virus code relates to this demo routine.

Copyright © Dr Solomon's Software

The virus also contains the following text, near the beginning:

```
WALKER 1.00 - This absolutely harmless and selfdestructive
program is written by UJHPTTLZ in the city of Istanbul, 1992
```

Warrior

Type

File virus.

Affects

EXE files on execution of an infected file.

File Growth

1,024 bytes.

Description

The text **`*.txt`** can be found in the virus. This is patched to **`*.exe`** at run time to search for files to infect.

While an infected program is running, any file-write will write the following message into the file instead. The message is:

```
... and justice for all! (US Constitution) Dream Over ... And
the alone warrior is warrior. The powerfull WARRIOR!
```

Werewolf (Claws, WeWo)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

See Variants.

Description

The first variants, **658-685**, infect EXE files only. Later variants are memory resident and infect both COM and EXE files. All variants are encrypted.

Copyright © Dr Solomon's Software

Werewolf.1500a-b variants add 6 seconds to the time-stamp of infected files. Infected COM files have 11 zero bytes, followed by 4 FF bytes at the end of file.

Werewolf.1500 intercept Int_21h and Int_13h. Interrupt 13h (disk i/o) is used for the payload. When a sector is written to disk, the virus changes a single byte in the sector, with an approximate probability of 3/100000. This results in very slow, and dangerous, corruption of data on the hard disk. This payload can be delivered at any time after infection, without any specific trigger-date.

Werewolf.1500a contains the following strings:

```
WULF

1996 WereWolf

TBMEMXXXTBCHKXXXTBDSKXXXTBFILXXX

CLEAN AVP TB V SCAN NAV IBM FINDV GUARD FV CHKDS F-
```

Werewolf.1500b contains the following strings:

```
TBMEMXXXTBCHKXXXTBDSKXXXTBFILXXX

[WULF]

CLEAN AVP TB V SCAN NAV IBM FINDV GUARD FV CHKDSK F-
```

Anti-virus programs containing the above strings are not infected.

Variants

658, 678, 684a-b, 685, 1152, 1168, 1208, 1361, 1267, 1500a-b.

Whale (Motherfish)

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

9,216 bytes.

Copyright © Dr Solomon's Software

Description

This virus is so large and clumsy that on most PCs it does not actually work at all. As a result, the main replication method has been anti-virus researchers sending specimens to each other. With careful treatment it can be persuaded to go memory resident and infect files. The system slows down considerably because the virus is so inefficient. It contains a few dozen 'heads' which are the different decryption/loader routines.

Winlamer

Type

File virus.

Affects

This virus infects executable files in the NE-EXE format (this is a format of 16-bit executables; most Windows 3.1 applications are in this format).

File Growth

Approximately 2,000 bytes.

Description

This is a direct action (that is, non-resident) virus; and the first Windows polymorphic virus.

Infected files are marked by adding 100 years to a current file time stamp, but this is not visible under DOS (the two high digits of the year are not displayed).

There is actually a problem, which explains why it took so long for a Windows polymorphic virus to appear. Under Windows, the code segment of the program is supposed to be write-protected. So, the code cannot modify itself and self-decrypting code (required for a polymorphic virus) is impossible. Nevertheless, this can be overcome if the request to get write access to a code segment is incorporated within the polymorphic decryptor. It is this approach which is used by ***Winlamer*** virus.

When the virus is started, the decryptor is run and it uses the DPMI API call (INT 31h/AX=000Ah) to duplicate a selector of a code segment. Then the virus assigns it to a data segment. At this point, the virus can write to this data segment, actually decrypting the virus body. This code is dissolved into meaningless garbage commands produced by the polymorphic generator of the virus.

Copyright © Dr Solomon's Software

After decryption the virus looks for all NE files in the \WINDOWS directory (if it is named differently it won't infect anything!) and infect them (this takes a noticeable time). Then control is passed to the host file.

The ***Winlamer*** virus has no payload.

Fortunately, the virus is not capable of infecting both normal DOS EXE files and NE files. If it were able to do this, it could (potentially) be much more virulent.

The virus was written by a prolific virus author, someone who calls himself "Burglar" from Taiwan. The virus contains the following strings:

```
Winlamer2 (C)Copyright Aug, 1995 by Burglar in Taipei.
```

and one more:

```
PME for Windows v0.00 (C) Jul 1995 By Burglar
```

Burglar is also the author of some other sophisticated viruses. In June 1995 he wrote **Wintiny.741**, a non-polymorphic NE-EXE infector. He also wrote the Phantasie Mutation Engine (PME), used both in his DOS and Windows viruses.

Winlamer was clearly an experimental virus and it was done just to demonstrate that polymorphism is possible for NE executables.

Wisconsin

Type

File virus.

Affects

A COM file on execution of an infected file. COMMAND.COM is avoided.

File Growth

852 bytes.

Description

If the year is not 1989, every fifth time an infected program is run it displays the message **`Death to Pascal`** and deletes every PAS file, displaying a dot as each file is deleted.

 Copyright © Dr Solomon's Software

Witcode

Type

Memory resident file virus.

Affects

EXE files on execution. If the virus tries to infect a write-protected disk the DOS **`Write protect error writing drive X: Abort, Retry, Ignore?`** message is displayed.

File Growth

966 to 981 bytes.

Description

While the virus is in memory, various effects are triggered on exit from any program, whether infected or not. Between 10 p.m. and 6 a.m., there is a 1-in-16 chance that the virus will display **`Gee, I wanna sleep now!.`** Between December 24th and 31st, it displays **`Merry Christmas!.`** On Sundays there is a 1-in-32 chance that it will display **`You really shouldn't work on Sundays....`**

On any Friday 13th and any Monday, there is a 1-in-64 chance of the payload triggering. This patches the first two bytes of the boot sector of drive C so that the hard disk becomes non-bootable.

WM.AntiDMV (AntiDMV,Date)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This virus is reportedly in the wild in Italy, Malta, Spain and probably in some other Mediterranean countries.

Copyright © Dr Solomon's Software

This virus was designed to spread until 1 June 1996; and should, therefore, have stopped spreading at this time. However, it is possible that many infected documents and templates may exist 'in the wild'.

WM.AntiDMV contains only one macro, AutoOpen. If an infected document is opened under Microsoft Word for Windows, the current year is before 1997 and the current month is before 6 June, the virus infects the global template, NORMAL.DOT. The virus also removes the macro AutoClose from documents and templates, if it exists.

It is the time limited feature, plus the removal of the AutoClose macro, which prompted the name of the virus; it effectively removes the *WM.DMV* virus.

WM.Atom (WordMacro.Atom, Atom)

Type:

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

The virus contains the macros AutoOpen, FileOpen, FileSaveAs, and ATOM (all execute-only).

When an infected document is opened, *WM.Atom* infects the global template. If NORMAL.DOT auto-macros are disabled, the virus is rendered ineffective. The virus does not turn off the prompting to save changes to the global template, so if prompting is turned on you will be prompted to save changes to the global template at the end of the Word for Windows session.

After the global template is infected, the virus calls its first destructive payload. If the current date is December 13th, the virus deletes all files in the current directory.

Once the virus is active (that is, it has infected the global template), it infects all documents which are saved using File/SaveAs, or which are opened using File/Open. If the seconds field of the current time is 13 at the time of infection, the virus encrypts the document being saved, with the password **'ATOM#1'**.

 Copyright © Dr Solomon's Software

WM.Colors (WordMacro.Colors, Colors)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

When an infected document is opened under Microsoft Word for Windows, the virus infects the global template, NORMAL.DOT. After this, every document being created using File/New, or saved using Save or File/SaveAs, is infected by the virus. The virus contains the following macros:

AutoOpen, AutoClose, AutoExec, FileNew, FileExit, FileSave, FileSaveAs, ToolsMacro and other macros.

If macros with such names existed prior to infection, they are overwritten by the virus.

Surprisingly enough, the AutoExec macro in the virus is an empty one - it does nothing. The possible aim could be to overwrite the existing AutoExec macro, which could contain anti-virus routines, for example, supplied by Microsoft.

The virus can propagate even with AutoMacros being disabled; for example, by invoking Word for Windows as WINWORD.EXE /mDisableAutoMacros or by using one of Microsoft's recent anti-virus template tools). As soon as a user chooses File/New, File/Save, File/SaveAs, File/Exit or Tools/Macro, the virus gets control and infects NORMAL.DOT. Moreover, unlike most other known Word for Windows viruses, ***WM.Colors*** virus cannot be recognized by using Tools/Macro to list the active macros. The virus intercepts Tools/Macro and effectively disables it, while still using it for infection. For this reason ***WM.Colors*** can be seen as the first macro virus with some stealth capabilities. However, File/Templates/Organizer/Macros can be used to view the names of the virus' macros, and even to delete them.

As with ***WM.Nuclear*** (the first encrypted macro virus), all macros in ***WM.Colors*** are 'execute-only' and thus cannot be viewed/edited using Word for Windows.

The virus also enables AutoMacros (in case the user had disabled it) and disables the Word for Windows prompt to save changes to NORMAL.DOT.

The virus maintains a counter called 'countersu' in the [windows] section of WIN.INI. Every time a virus macro is called (with the exception of AutoExec) the

Copyright © Dr Solomon's Software

counter is incremented by one. Thus, every time a user opens, creates, saves, closes a document, attempts to use Tools/Macro or exits Word for Windows, the counter is incremented. When the counter reaches 299, and each 300th time thereafter (that is, 299, 599, 899 and so on), the virus triggers. Then it changes the Windows color settings (text, background, buttons, borders, and so on) to randomly-selected colors.

WM.Colors.B (Colors.B)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File growth

-

Description

In early April 1996 a prominent anti-virus researcher investigated what at first appeared to be an outbreak of the ordinary ***WM.Colors*** macro virus, in Portugal. When a sample of the virus involved was examined he discovered that it contained the ***WM.Colors*** virus, except that the macro replacing AutoOpen was not from ***WM.Colors***, it was the one found in ***WM.Concept***!

One likely explanation of what happened is that a machine infected with ***WM.Colors*** was then exposed to a document infected with ***WM.Concept***. When the other code in ***WM.Colors*** caused it to replicate, it copied the ***WM.Concept*** version of the AutoOpen macro to the target instead of its own AutoOpen, without checking. In any case, the virus still replicates in its new form.

WM.Concept (WinWord.Concept, WW6Macro, WW6Infector, WBMV (Word Basic Macro Virus), Prank Macro, Concept)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

 Copyright © Dr Solomon's Software

File Growth

-

Description

This was the first virus to infect data files. *WM.Concept* infects Word for Windows 6 documents (*.DOC) and the NORMAL.DOT template. The virus makes use of the well-developed Word for Windows macro language, Word Basic, in an attempt to exploit the fact that PC users exchange documents far more often than programs.

When an infected document is opened under Word for Windows for the first time, the virus gets control as an AutoOpen macro and infects the NORMAL.DOT template (or any other template, if it has been selected as a global default template). A Word for Windows message box, with the text `'1'`, appears on the screen. After this, every document saved using the File/SaveAs command is infected with the virus. Normally this happens when a newly-created document is saved to the disk.

If Word for Windows is run, then Tools/Macros is selected and the list of macros checked, the presence of the macros called AAAZFS, AAAZAO, AutoOpen, PayLoad and FileSaveAs indicates that the Word for Windows system is infected with *WM.Concept*.

This virus works under versions of Microsoft Word for Windows 3.x, Windows 95, Word for Windows NT and Macintosh. Like other macro viruses WM.Concept is not platform specific.

WM.Concept.B.Fr (Concept.B.Fr)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

In early March 1996, someone translated the FileSaveAs macro, called *WM.Concept*, into the French equivalent, producing a French-only version of *WM.Concept.* This infected a large site within France. The translated macro name is the only difference between it and the original *WM.Concept*.

Copyright © Dr Solomon's Software

WM.Divina (Divina)

Type

Microsoft Word for Windows documents.

Affects

See description.

File Growth

-

Description

Like *WM.DMV, WM.Divina* virus contains just an AutoClose macro; this is execute-only. When an infected document is loaded under Microsoft Word for Windows and then closed, the virus infects NORMAL.DOT. Any document closed after this will be infected.

The virus has two payloads.

(1) If a document is being closed during the 17th minute of any hour, a set of dialog boxes are displayed, with pauses and beeps in between. The first says

```
ROBERTA TI AMO!
```

Next comes

```
Exit from system and low level format are recommended.
```

and finally

```
Exit from System?
```

After this the virus exits Windows. So, while the virus has no destructive payload as such, it might well succeed in persuading an average user to re-format his/her hard disk.

(2) Another payload triggers on 21st May, if a document is being closed between 10th and 20th, or between the 40th and 50th minute of any hour. Two dialog boxes are displayed:

```
DIVINA IS THE BEST!
```

followed by a box titled "Virus 'DIVINA' in esecuzione", and containing some message in Italian. After this the virus exits Windows.

Judging by the language, style, variables and sub-routine names, it is certain that *WM.Divina* was written by the same person who wrote *WM.AntiDMV.*

 Copyright © Dr Solomon's Software

WM.AntiDMV is fairly widespread in Italy, Malta and Spain [but should have stopped replicating after 1 June 1996]. Thus, AntiDMV could in fact be 'WM.AntiDivina'.

WM.DMV (DMV)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

We believe that this virus was written for 'demonstration' purposes by an American computer user. Subsequently, he made the virus available for all to download via the World Wide Web.

The author of this virus also attempted to write a Microsoft Excel for Windows macro virus - but it fails to work because of a bug.

WM.Extra (Clock)

Type

Macro virus.

Affects

Microsoft Word for Windows documents by use of Word for Windows macros.

File Growth

-

Description

WM.Extra's macros are encrypted (execute-only). Although the virus was written for the German version of Word for Windows, it still replicates under other language versions.

The virus has an demonstrative, but innocent, payload. If the following conditions are met:

Copyright © Dr Solomon's Software

year > 1996

minute > 39

day > 25

the virus displays the digital clock every two minutes.

WM.Extra includes the following macros (the length, in bytes, is given in brackets):

ACTION (1168)

ÖFFNEN (200)

AUTOEXEC (333)

AUTOOPEN (322)

SPEICHERN (210)

EXTRASMARKO (13)

DATEISCHLIEßEN (101)

DATUMUNDUHRZEIT (241)

DATEIDOKVORLAGEN (13)

DATEIALLESSPEICHERN (78)

DATEISPEICHERNUNTER (1116)

WM.Friendly (Friendly)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File growth

-

Description

This virus, German in origin, was discovered in mid-May 1996. It shows signs of having been written by the same person as *WM.Telefonica*. It creates an INI file entry [friends] in which it sets

```
Author=Nightmare Jocker
```

 Copyright © Dr Solomon's Software

It attempts to be bi-lingual by containing a complete set of its macros in English, as well as a complete set in German!

Unfortunately for the author, who apparently did not have a copy of Word for Windows in English to test the virus, his English set of macros are improperly saved. As a result the virus does not work under the English version after all.

When it replicates under the German version of Word for Windows, it plants a copy of a variant of the old DOS virus, 'Little Brother'.

WM.FormatC (FormatC)

Type

Macro trojan.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This is not a virus, but a trojan. It does not replicate. Its payload is to format drive C as soon as the document is opened. It uses an undocumented feature of FORMAT; if /AUTOTEST is added to the command line the usual warning message given by FORMAT is not displayed. This trojan was posted to a Usenet newsgroup.

WM.Guess (Guess)

Type

Macro virus.

Affects

See description.

File Growth

-

Description

This is a multi-language macro virus, first seen in Germany in May 1996. It replicates via a single macro, AutoOpen, which is language independent.

Copyright © Dr Solomon's Software

When decrypted it appears to have been written by high school children. It displays some silly messages, including **`Hi sexy!`** and **`Guess who?`**

WM.Hot (Wordmacro.Hot, Hot)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This virus creates an entry in the WINWORD6.INI configuration file. This contains a 'hot date', 14 days in the future, when its payload will trigger.

The virus activates randomly within a few days of the 'hot date'. When the user tries to open a document its contents are erased instead.

The payload is disabled if the file C:\DOS\EGA5.CPI is found to exist. A comment in the virus source code suggests that this is a 'feature' designed to protect the virus author and the author's friends.

WM.Imposter (Imposter)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This virus, very closely related to *WM.Concept*, was discovered in England at the beginning of March 1996.

 Copyright © Dr Solomon's Software

It contains code similar to that found in both the *WM.DMV* virus and in *WM.Concept*. In fact one of its macros is always named DMV. Like *WM.Concept*, it contains a Payload macro, but this one says **`just to prove another point`**.

It was named *WM.Imposter* due to its attempt to appear as either *WM.DMV* or *WM.Concept* and hopefully fool anti-virus products, an attempt at which it is generally unsuccessful.

WM.NOP (WordMacro.Nop, WinWord.Nop, Nop)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

WM.NOP is 'in the wild' in Germany.

In order to spread, this virus requires the German version of Microsoft Word for Windows 6.0 or above; under other language versions of Word for Windows, the virus will infect NORMAL.DOT but will not spread further.

Documents infected with *WM.NOP* contain the macros AutoOpen and NOP. When an infected document is opened under Word for Windows, the virus gets control via the AutoOpen macro and infects the NORMAL.DOT global template. In an infected NORMAL.DOT, the AutoOpen macro becomes NOP and the NOP macro becomes DateiSpeichern (German for FileSave).

WM.NOP has no payload.

WM.Nuclear (Nuclear)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

Copyright © Dr Solomon's Software

File Growth

-

Description

When an infected document is opened, the virus infects the NORMAL.DOT template. After this, every document saved using File/SaveAs is infected with the virus. Unlike the ***WM.Concept*** virus, all macros in ***WM.Nuclear*** are 'Execute-Only', that is, they are protected (encrypted) so that you cannot view or modify their source code, but you can view the macro names with Tools/Macro.

Infected documents (or template NORMAL.DOT) contain the following macros: AutoOpen, AutoExec, DropSuriv, FileExit, FileSaveAs, FilePrint, FilePrintDefault, InsertPayload, and PayLoad.

If a document is being printed, and the system clock seconds-counter is between 55 and 59 seconds (that is, with a probability of approximately 1/12) the following lines are added to the document, and are printed subsequently at the end of the last page:

```
And finally I would like to say:

STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!
```

The virus also has side-effect of causing error messages when using Cancel from File/Print or File/SaveAs.

The virus was also supposed to drop a 'normal' virus, that is, infecting COM, EXE and New EXE files, and called ***PH33R*** (fear). However, due to a number of bugs, it fails to achieve this effect. Another destructive payload intended by the author was designed to trigger on 5th April, in any year. This Payload macro was meant to damage (truncate to 0 bytes) the system files IO.SYS, MSDOS.SYS and COMMAND.COM. Fortunately, this also does not work, due to bugs in the code.

Variants

a - b.

WM.Nuclear.B (Nuclear.B)

Type

Macro virus.

Affects

MicroSoft Word for Windows documents.

Copyright © Dr Solomon's Software

File Growth

-

Description

This is a variant of *WM.Nuclear* apparently, altered from the original virus by some curious and inept user messing around with it. This virus was discovered in a corporation in France in early March, 1996.

Since the original *WM.Nuclear* virus was encrypted, it is likely that the user obtained the unencrypted source code from where it was posted (to an Internet newsgroup created for the distribution of viruses and the promotion of virus writing) and worked from that to create this new variant.

WM.Nuclear.B does not try to plant the *PH33R* virus but instead calls other destructive routines from the original virus at that point.

This variant does not replicate in encrypted form, so it will be much easier for others to learn from and it is expected that advanced macro virus programming techniques from this virus will start showing up much more often in future viruses.

WM.Polite (Polite)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

WM.Polite was discovered in the USA, in late March 1996. It installs only FileClose and FileSaveAs replacement macros, and so avoids detection by systems watching Auto macros.

It is rather odd in that it asks each time before it infects a document. Unfortunately, it does not ask when it originally infects the Global Template. It is not expected to survive and spread well in the wild.

Copyright © Dr Solomon's Software

WM.Telefonica (LBNYJ)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

Discovered in late April 1996 this is a German Word for Windows specific macro virus. It tries to create and execute an encrypted COM file (using DEBUG) in 1 out of 60 infections.

It replicates using MacroCopy to replicate its set of seven macros, including FileNew, FileOpen, FileClose, AutoOpen and Autoexec.

This virus was first reported attached to a document which was an order form in German for a set of erotic videos.

WM.Wazzu (WinWord.Wazzu, WordMacro.Wazzu, Wazzu)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This virus contains only one macro, AutoOpen. Since the name of the AutoOpen macro is the same in all versions of Word for Windows, this is the first virus that will replicate equally effectively in all language versions of Word for Windows. This virus is quite widespread.

Variants

a-f.

Copyright © Dr Solomon's Software

WM.Wiederoffnen (Wiederoffnen)

Type

Macro trojan.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This is not a virus, but a Word macro trojan. It comes in a Microsoft Word for Windows 2 document but also works perfectly under Word for Windows 6. *Wiederoffnen* intercepts the AutoClose macro and when the document is closed plays tricks with AUTOEXEC.BAT.

WM.Xenios (Xenios, Nemesis, Evil One)

Type

Macro virus.

Affects

Microsoft Word for Windows documents.

File Growth

-

Description

This virus was distributed in a file named NEMESIS.ZIP on an internet newsgroup back in February 1996 and so has received broad initial distribution.

Its further spread has been somewhat limited by the fact that it was written to exploit only the German language version of Microsoft Word for Windows. It will infect the Global template file of an English Word for Windows user but will not replicate further into new documents.

While it is active, it watches for attempts to print files and about half the times this happens it adds the phrase **`Brought to you by the Nemesis Corporation c 1996`** onto the end of the document being printed.

Copyright © Dr Solomon's Software

When files are saved the virus encrypts them with the file password 'xenicos' just over half the time. ***WM.Xenios*** replaces the Tools/Macros command with code that will display an error message instead of activating Word's built-in macro viewer/editor, so it is not so easy to see its macros are in place.

One other interesting effect is that ***WM.Xenios*** tries to plant, and arrange to activate, a variant of the DOS multipartite virus known as ***Neuroquila*** when files are saved after March 1. It succeeds in planting this DOS virus but not in running it. The ***Neuroquila*** variant planted contains a bug so it only infects boot sectors and not programs.

AUTOEXEC.BAT is altered to call the ***Neuroquila*** virus.

Wolfman

Type

Memory resident file virus.

Affects

COM and EXE files.

File Growth

2,064 bytes.

Description

The virus contains the text **`Wolf_mAN`**.

On the 15th of the month the payload triggers. This is supposed to overwrite the hard disk, but it just hangs the system.

WW-217

Type

File virus.

Affects

A COM file on execution of an infected file.

File Growth

217 bytes.

 Copyright © Dr Solomon's Software

Description

The last two bytes of an infected file are **WW**.

Variants

WW217a is a minor variant.

WWT-01

Type

Overwriting file virus.

Affects

All COM files in the same directory on execution of an infected file. Date/time and read/write attributes are not preserved.

File Growth

None. The first 67 bytes are overwritten.

Description

Programs no longer function.

Variants

WWT-02:

125 bytes are overwritten. Date/time and read/write attributes are preserved.

WXYC

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Copyright © Dr Solomon's Software

Description

WXYC is a boot sector virus infecting the boot sector of hard disks and the boot sector of floppies. *WXYC* is unusual in this regard as most boot sector viruses infect the partition sector rather than the boot sector of hard disks. The hard disk is infected when the PC is booted from an infected floppy disk. Any floppy disk accessed in an infected PC is infected with the virus.

The original DOS boot sector is stored on cylinder 0, head 0, sector 3 of the hard disk.

The virus does not use stealth techniques to hide itself. Sometimes (this depends on the time) the virus displays **`WXYC rules this roost!`** when the computer is re-booted.

There is a string inside the virus body which never gets displayed: **`'JAM WXYC'`**. This is used by the virus for self recognition.

Variants

a-b.

XA1 (Tannenbaum, Weinacht)

Type

File virus.

Affects

A COM file in the current directory on execution of an infected file. Only files between 7 and 63,487 bytes are infected. Date/time and read/write attributes are preserved. IBMBIO.COM and IBMDOS.COM are avoided.

File Growth

1,539 bytes.

Description

On April 1st the partition sector of the hard disk is replaced with the virus code, which also replaces the boot sector on drives A and B. Thereafter, when the PC is started the message **`April, April ...`** is displayed, then the PC beeps and hangs.

Between December 24th and 31st it displays a Christmas tree and the message **`Und er lebt doch noch : Der Tannenbaum! Frohe Weihnachten ....`**

This was found in Germany, hence the language. The April message is the equivalent of April Fool, and the other message (Christmas Tree! And it lives still) may be a

 Copyright © Dr Solomon's Software

reference to the Christmas exec worm which went through the IBM network at the end of December 1987.

Xeram

Type

File virus.

Affects

COM and EXE files.

File Growth

-

Description

The virus is not memory resident. It has no stealth capability and is very visible. The whole virus is encrypted, and it has a variable loader. The virus displays a message.

Variants

1664.

Xmas

Type

File virus.

Affects

COM or EXE files on execution of an infected program.

File Growth

2,764 to 2,779 bytes.

Description

If an infected file is run on December 25th, occasionally a Christmas message will be displayed. This consists of **M E R R Y C H R I S T M A S !** at the bottom of the screen and four lighted candles. At the same time it plays the Tannenbaum carol. In the run-up to Christmas, the number of lighted candles increases from one to four.

This virus is another version of ***Syslock***.

Copyright © Dr Solomon's Software

XM.Laroux (Laroux)

Type

Macro virus.

Affects

Microsoft Excel for Windows spreadsheets.

File Growth

-

Description

WM.Laroux is the first macro virus for Microsoft Excel for Windows which actually works. The virus intercepts Excel's AutoOpen automacro. When an infected spreadsheet is opened, the virus activates and checks whether the system is already infected. If not, the virus creates an Excel for Windows file named PERSONAL.XLS in the Excel for Windows default startup directory (e.g. C:\MSOFFICE\EXCEL \XLSTART) and copies itself there. The spreadsheets and macros from that directory are automatically loaded whenever Excel for Windows is run. From then on, every spreadsheet being opened or created on an infected system will become infected with the virus.

This virus does not have an intentional payload - it just replicates. The virus works under Excel for Windows versions 5 and 7, running under Windows 3.x, Windows 95 and Windows NT. It does not work on Apple Macintosh.

Infected spreadsheets contain a hidden sheet named 'laroux'. Here is a fast check to tell whether you have the virus:

If Tools/Macro is used to view the macros associated with a spreadsheet, the macros 'auto_open' and 'check_files' and/or 'personal.xls!auto_open' and 'personal.xls!check_files', indicates that the system is infected.

XPEH.4016 (XPEH, XPEH4, XPEH5, Micropox)

Type

Memory resident file virus.

 Copyright © Dr Solomon's Software

Affects

COM and EXE files on execution or search via DOS Find First/Find Next calls. COMMAND.COM, AIDSTEST.EXE (a popular Russian anti-virus program), and COM files of less than 288 bytes and greater than 61,815 bytes are not infected.

File Growth

4,016 bytes.

Description

This virus uses several layers of complex self-encryption and demonstrates certain anti-bugging techniques. The name XPEH is, in fact, in Cyrillic and is pronounced 'hren'. This is Russian for 'horse radish', but is often used in Russian swearing to mean something rather different.

The virus was designed not to activate until March 1991, being, presumably, distributed passively before this date, for example, by software copying and downloads from a BBS. Due to a bug, the virus is inactive in January and February of any year. At other times, on execution of an infected program the virus goes memory resident and there is a 1-in-4 chance that it will infect COM and EXE files being executed or looked for with the DOS Find First/Find Next calls.

The virus is a semi-stealth virus – the increase in file size of infected files is concealed if the virus is memory resident.

Starting in September 1991, if a file with no extension, or an extension of BAK, LEX or TXT is found via the DOS Find First/Find Next calls, the virus can trash the file's contents on approximately 1-in-4 occasions. Every four consecutive bytes of a trashed file are XORed with the hex pattern 90958D85, which stands for XPEH in the Russian alternative Cyrillic character coding.

Variants

There are eight known variants. They differ in activation and trigger dates, file growth, and encryption complexity. Some do not trash text files and are able to infect COMMAND.COM.

One of the latest variants contains the following encrypted Russian message:

```
Further development of XPEHs is suspended due to the virus
author getting a permament job.
```

Copyright © Dr Solomon's Software

Yale (Alameda, Merritt, Peking, Seoul, Yale Boot)

Type

Boot sector virus.

Affects

The boot sector of floppy disks and the partition sector of hard disks, when the PC is booted from an infected floppy disk.

File Growth

-

Description

When the PC is booted from an infected floppy disk (not necessarily a bootable one), the virus goes memory resident. When the disk is replaced and Ctrl Alt Del is pressed, the keystrokes are intercepted and the replacement disk is infected. The virus occupies 1Kb of RAM.

The original boot sector is moved to cylinder 39, side 0, sector 8. Any data is overwritten. The virus contains code for formatting cylinder 39, but an essential part is missing in all known versions so the format does not happen.

Yankee-1202 (AF00-1202)

Type

Memory resident file virus.

Affects

COM and EXE files on execution. Files must be greater than 6,144 bytes, and COM files must be less than 63,822 bytes.

File Growth

1,202 bytes.

Description

There is no payload.

 Copyright © Dr Solomon's Software

Yankee Doodle (Vacsina, YD.TPXX)

Type

Memory resident file virus.

Affects

COM files on loading. EXE files less than 63Kb are first converted to COM files (without a name change) and then infected the next time they are executed. Read/write attributes are preserved, but date/time is not preserved.

File Growth

COM: 1,207 to 1,213 bytes. Converting EXE to COM files grows them typically by 132 bytes.

Description

When a file is infected drive A is accessed, even if the infected program is not accessed.

There is no payload, other than a beep when a COM file is infected.

Variants

There are 16 versions, each with a different file growth, including several *Vacsina* variants. There is little functional difference from the original.

In the case of the *Vacsina* variants, the virus goes memory resident when an infected COM or EXE file is run. Any program which is run while the virus is in memory will be infected. Infected files grow by between 2,772 and 2,900 bytes. Date/time is preserved. If the virus is in memory at 5 p.m., the virus plays the tune 'Yankee Doodle'.

Yukon

Type

Overwriting file virus.

Affects

All COM files in the same directory on execution of an infected file.

File Growth

None. The first 151 bytes are overwritten.

Copyright © Dr Solomon's Software

Description

Infected programs no longer work.

The virus contains the text **`Divide Overflow`** which is displayed when an infected file is run. The program then exits.

Zero-hunt1 (Minnow)

Type

Memory resident file virus.

Affects

COM files on execution.

File Growth

None.

Description

The virus attempts to use stealth to hide its infection of a file by filtering out the virus code when a program tries to read an infected file. If the virus mistakes an uninfected file for an infected one, reading that file will give the wrong results.

Zero-hunt2

Type

Memory resident file virus.

Affects

A COM file when a directory change is made.

File Growth

None. Overwrites 416 bytes.

Description

The virus looks for a group of 416 zeros, then overwrites these with itself. If the virus is in memory it conceals the change by re-substituting the zeros when the file is read.

 Copyright © Dr Solomon's Software

Zero-to-O

Type

Overwriting file virus.

Affects

A COM file on execution of an infected file.

File Growth

None. Overwrites 403 bytes.

Description

Programs no longer work.

Each time a program is run, every 0 (zero) on the screen is converted to the letter O, unless the screen is mono, in which case the system hangs.

Zero Bug (Zero Eater, Zbug)

Type

Memory resident file virus.

Affects

Any copies of a COM file during creation. The read/write attribute is preserved.

File Growth

1,536 bytes.

Description

The virus uses stealth to conceal the increase in file size when it is memory resident. The virus triggers a screen display with a face (ASCII character 1) eating all the zeros, starting at the top left and working its way down from left to right. Zeros are replaced by spaces.

Zerotime (V1721, Slow, Sydney)

Type

Memory resident file virus.

Copyright © Dr Solomon's Software

Affects

EXE and uninfected COM files on execution. Date/time and read/write/hidden attributes are preserved on COM files. COMMAND.COM is avoided.

File Growth

COM: 1,721 bytes.

EXE: rounded to a multiple of 16 bytes, then another 1,716 bytes are added.

Description

Some EXE files are not infected correctly and fail to run.

Every Friday in 1991 and after, whenever any file is closed the file time-stamp is set to zero. It looks as though the author intended the date to be set to zero as well, but it is set to whatever is in the DX register. This usually means the date is zeroed, but not always.

This is a variant of ***Jerusalem***, with variable encryption. Misinfections of EXE files are possible because of the faulty way in which the virus distinguishes between COM and EXE files.

Zherkov

Type

Memory resident file virus.

Affects

COM and EXE files on execution or opening. Only files less than 64,512 bytes are infected.

File Growth

1,018 to 2,970 bytes.

Description

The strings **`Welcome to demo version (C) Zherkov`** and **`AIDSTEST`** can be found in the virus, and the whole virus is encrypted.

If any floppy disk is formatted in drives A or B, the BIOS Parameter Block will be patched to reflect zero heads. If you access a floppy disk this will be concealed so that the BIOS read gives two heads. The same disk may not work on an uninfected PC because of the error in the BIOS parameter block.

 Copyright © Dr Solomon's Software

If a program called AIDSTEST.EXE (a popular Russian anti-virus program) is run, the message **`version (C) Zherkov`** is displayed and the file deleted.

Variants

1010, 1023, 1882, 1915, 1958, 2968, 2960.

ZK900 (France, Death March)

Type

Memory resident file virus.

Affects

COM and EXE files on execution.

File Growth

900 bytes.

Description

Seventy-three seconds after infecting, the virus plays the Death March, repeating it every three minutes.

Copyright © Dr Solomon's Software

 Copyright © Dr Solomon's Software

Glossary

alias	A different name by which a *virus* is known.
AHA	Advanced Heuristic Analysis. A technique using a *heuristic scanner* in FindVirus to scan a file for suspicious code and algorithms.
AT	A PC based on the 80286 processor or better.
ASM	Anti-Stealth Methodology. A feature of some programs in the Anti-Virus Toolkit, used as an additional safety measure against viruses using stealth.
AUTOEXEC.BAT	A *batch file* that specifies a set of commands that are executed every time you start the PC.
backup	A copy of your data held in another place in case your working copy is lost or damaged.
batch file	A file containing a set of DOS commands that you can run by typing just one command. Batch files have the file extension BAT.
BBS	Bulletin Board System. An electronic mail system used to send messages and transfer files.
BIOS	Basic Input/Output System. Permanent programs that are used to load DOS when the system is started up.
boot	Start the computer.
boot disk	A floppy disk containing operating system files which can be used to start the PC.
boot sector	One of the system areas on hard disks

Copyright © Dr Solomon's Software

	and floppy disks containing code which is executed whenever the PC is started from the PC.
boot sector virus	A virus which infects the boot sector of floppy disks. If the PC is started with an infected floppy disk in drive A, the virus will normally infect the partition sector of the hard disk (though some infect the boot sector of the hard disk).
bug	An unintentional fault in a program.
caching	A way of reducing the amount of time a program spends accessing the hard disk. Part of the memory is used as a temporary store.
CARO	Computer Anti-Virus Researchers Organisation. Dr Solomon's has several CARO members.
checksummer	A program that looks for viruses by checking for changes to *executable files*. ViVerify is an example of a checksummer.
clean	Free from viruses.
cluster	The minimum allocation unit on a disk, usually consisting of 2, 4, 8, 16 or 32 *sectors*.
CMOS	An area of storage used to hold system setup details in PCs with a 286 processor or above. CMOS is non-volatile memory, which means that its contents are not lost when the PC is powered off.
cold reboot	Rebooting the system by turning off the PC and turning it on again. This is normally recommended when before scanning for viruses as some viruses can survive a *warm re-boot*.
COM file	An *executable file* with a COM

Copyright © Dr Solomon's Software

	extension.
COMMAND.COM	The DOS command interpreter which processes the commands typed in by the user.
command line	Allows programs to be run by the user typing a specific command rather than using a mouse, or user-interface, to select programs.
compressed file	A file that contains a packed copy of an original file or files, designed to save disk space. Files are compressed using a 'zip' utility, for example, PKZIP, and the file must be decompressed (for example, with PKUNZIP) before the files within the compressed file can be used. Another form of file-compression is a self-extracting archive file, which is decompressed automatically when the compressed program is run.
CONFIG.SYS	A file in the root directory which specifies which devices to install and which *device drivers* to use.
conventional memory	Memory in a PC available for running DOS applications; programs executed under DOS are able to run only in the first 640Kb of memory. Also know as base memory.
cylinder	All the *tracks* on a disk which are the same distance from the centre.
device driver	A DOS program used to control the items of hardware connected to the PC, for example, disk drives and printers. Some device drivers are built into DOS, and others are added as device = commands to CONFIG.SYS.
directory	A logical sub-division of a disk which organizes files into groups. DOS holds information on files within a directory which can be displayed using the DIR

Copyright © Dr Solomon's Software

	command.
disk compressor	A program which stores files in a compressed form to maximize space on the hard disk.
dropper	A file which is not itself a virus, but which contains virus code which is 'dropped' onto the hard disk.
driver file	A file used by Toolkit programs to enable the identification and removal of viruses.
EICAR	European Institute for Computer Anti-Virus Research.
eof	End of file.
enhanced memory	Memory installed on the PC in addition to *conventional memory*, either as extended memory or expanded memory.
EXE file	An *executable file* with an EXE extension.
executable file	A program file, containing executable instructions.
expanded memory	A type of memory which can be installed in addition to *conventional memory*. Available on 286-based PCs and above. Commonly known as EMS.
extended memory	A type of memory which can be installed in addition to *conventional memory*. Commonly known as XMS.
false alarm	A report of a virus where none exists.
fast infector	A memory-resident virus that infects programs when they are opened or copied, or when they are run (most viruses infect only when the programs are run).
FAT	File Allocation Table. The area on a disk

Copyright © Dr Solomon's Software

	which holds information on which *clusters* on the disk belong to which file.
file virus	A virus which infects *executable files*. When the program is run the virus is executed also. Most file viruses are *memory-resident*.
fingerprint	A unique numeric identifier for a file. Used by *checksummers* to check for changes in executable files. Also known as a checksum.
footbath PC	A PC used to check incoming files and disks for viruses. Also known as a *sheep-dip PC*.
format	The method of preparing a disk before use, using the DOS FORMAT command. The command creates a *root directory* and a *FAT*.
GDE	Generic Decryption Engine. An element of FindVirus which enables it to identify and remove even the most complex polymorphic viruses.
head	One of the read/write coils in a disk drive.
heuristic scanner	A program which uses the characteristics of a file to determine whether or not it is likely to be a virus.
hexadecimal	Numeric representation in base 16.
HPFS	High Performance File System. The file system used by the operating system OS/2.
in the wild	A term used by virus researchers to describe any virus that has infected a computer and that has been reported outside a virus research site.
infected file	A file containing a virus.
Internet	A world-wide network of millions of

Copyright © Dr Solomon's Software

	computers. Provides access to a wide variety of information through web sites.
interrupt	The way in which requests are made to DOS and the *BIOS* to perform tasks on a PC.
joke programs	These are not viruses, but sometimes a virus is contained in a joke program. FindVirus detects some common joke programs.
logic bomb	A type of *trojan* that is triggered by a particular set of circumstances.
low-level format	A *BIOS*-level format. Unlike a DOS format, this erases all the contents and partition information of a hard disk. Most modern hard disks cannot be low-level formatted easily.
macro	Executable instructions associated with the data files of some word processors. If the macro language used to create macros is sufficiently powerful, *macro viruses* can be written, which spread via the use of data files.
macro file	A data file containing instructions that specify actions to be taken by an applications program.
macro virus	Any virus, similar to the ***WM.Concept*** virus, that infects data files, for example, Word for Windows document files.
MBR	Master Boot Record. The *partition sector* of a hard disk.
memory-resident	A program which remains in the PC's memory once it has run. Also known as *TSR*. See also *VxD*.
multipartite virus	A virus which uses a combination of techniques to spread, for example,

Copyright © Dr Solomon's Software

	infecting both files and *boot sectors*.
NLM	NetWare Loadable Module. A program designed to run under the Novell NetWare operating system.
NTFS	New Technology File System. The file system used by the Windows NT operating system.
overwriting virus	A virus which overwrites each file it infects.
partition sector	The first sector of a hard disk. The executable code in this sector is for whenever the PC is booted from the hard disk. The partition sector also contains the partition table, which specifies the number of sectors on the disk, information on each partition (or volume) and the location of the *boot sector*.
partition sector virus	A virus that infects the *partition sector*.
payload	What a virus does when it triggers.
polymorphic virus	A virus that tries to evade detection by scanners by ensuring that it does not have a fixed pattern of bytes. FindVirus can detect polymorphic viruses using the Generic Decryption Engine.
public domain software	Software which you can copy and distribute legally.
RAM	Random Access Memory. Amount of RAM is measured in bytes, kilobytes (Kb) and megabytes (Mb).
RAM drive	An area in memory which emulates a hard disk drive, but provides faster access.
rescue disk	A disk used to restore the *partition sector*, *boot sector* and *CMOS* of your hard disk if they have been infected by a virus.

Copyright © Dr Solomon's Software

root directory	The topmost directory on a disk, where all other directories and files are stored.
scanner	A virus detection program that searches for known viruses. FindVirus is an example of a scanner.
sector	Part of a *track*, usually 512 bytes long.
shareware	Software which you can copy legally, but must pay for if you decide to use it.
sheep-dip PC	A PC used to check incoming files and disks for viruses. Sometimes called a *footbath PC*.
stealth	Characteristic of a virus which tries to avoid detection. Stealth viruses interfere with DOS and *BIOS interrupts* in order to conceal their presence when they are memory-resident.
SYS file	File, generally a *device driver*, with a SYS extension.
time bombs	A type of *trojan*, triggered by a particular date.
track	All the *sectors* around the disk on a single *head* and at a the same distance from the centre. Referred to also as a cylinder.
trigger	the condition(s) which cause a virus to deliver it's payload (for example, date, number of re-boots, etc.)
trojan	A program that has an unexpected action. Trojans are not viruses, as they do not replicate, but they are often damaging. The Toolkit programs detect known trojans.
TSR	Terminate and Stay Resident. A program that remains in memory after it has run.
upgrade	A new version of the Toolkit which has

Copyright © Dr Solomon's Software

	been updated to detect newly-discovered viruses. Upgrades are available quarterly or monthly.
variant	A variation of a virus, usually caused by a change to the code of an existing virus.
virus	A program that replicates itself.
VxD	Virtual Device Driver, the Windows equivalent of a *TSR*.
warm re-boot	Restarting the PC by pressing Ctrl Alt Del at the same time. Some viruses, for example, ***Joshi***, can survive a warm re-boot.
write-protect	Ensuring that files cannot be written to a disk. A 5¼" disk is write-protected by placing a label over the notch. A 3½" disk is write-protected by sliding a plastic tab to uncover a hole.
XT	PC based on the 8086 processor.

Copyright © Dr Solomon's Software

 Copyright © Dr Solomon's Software

Index

Numerics
10 Past 3 59
100 Years 143
10AM 214
1232.a. Samsoft 186
1392 64
15 Years 129
1-in-8 322
2Kb 179
3APA3A 58
3tunes 303
648.re-boot.a 323
648-Lisbon 193
732 271
9.8min 185

A
Adin 83
Advanced Heuristic Analysis 37
Advanced stealth 46
AF00-1202 358
Agiplan 212
Ahav 60
Aids 60
Aids Information Diskette 27
Aija 138
Aircop 61
Aircop.Standard 61
AircopNGa-c 61
Aircot 61
Akuku 61
Akuku.b 61
Akuku.c 62
Alabama 62
Alabama.a-b 62
Alabama.b 62
Alameda 358
Alfons 62
Alfons.1344 63
Alfons.1536 63
Ambulance 63
Amoeba 64
AMSE NopB 285
AMSE NopB2 285
Amz.789 281
Anarkia 173
Angelina 64
Anthrax 65
Anticad 65
Antichrist 207
AntiCMOS 66
AntiCMOS.a 66
AntiCMOS.b 66
AntiDMV 337
AntiEXE 67
AntiEXE.a 67
AntiEXE.a-d 264
Anti-Pascal 68
AntiTel 183
Anti-virus software 16
Anti-virus tools 17
AP-400 68
AP-440 68
AP-480 68
AP-529 68
AP-605 68
Arab 68
ARARA 69
Arianna 69
Arianna.3375 70
Arianna.3426 70
Armagedon 70
Armee 292
Association of Really Cruel Viruses 33
AT144 70
Athens 310
Atom 338
Attention 71
Australian 286
Austrian 322
Avispa.2048 71
Avispa.2048.a-f 72

Copyright © Dr Solomon's Software

Azusa.a 287
Azusa.d 284

B
BackFont 72
Backfont-905 72
Backtime 72
Bad Boy 73
Bad Boy.a 73
Bad Boy.b 73
Bad Guy 74
Badsec 74
Badsec.3422 74
Badsec.3428 74
Bandit 75
Barrotes 75
Barrotes.1127 76
Barrotes.1194 76
Barrotes.1303 76
Barrotes.1310 76
Barrotes.1874 76
Barrotes.849 76
Barrtoes.1463 76
Batman 76
Bebe 77
Beeper 264
Beijing 77
Best Wishes 77
BestWishes 1 78
Bhaktivedanta 291
Big Italian 244
BigMouse 227
Black Avenger 107
Black Friday 172
Black Hole 172
Blink 140
Bloody 180
Bloody! 286
Bloomington 225
Boot sector viruses 6
Boot-c 256
Bosnia 82
Bouncing Ball 243
Bouncing dot 243
Boys-500 83
Boza 83
Bravo 287
Breasts 273
Brunswick 286
Buchanan, John 33
Bugs 2
Bunny.a 287
Bupt 9146 77
BuptBoot 77
Burger, Ralf 21
Burger-Pascal 231

C
Campana 297
Canadian 128
Cansu 318
Carfield 175
Cavaco 266
Central Point 29, 35
Centry 96
Century 143
Chance.B 96
Changsha 96
Changsha.3072 97
Changsha.a 97
Chaos 97
Chaos.1241 97
Charlie 322
Charlie virus 21
Checksummers 18
Chill.554 97
Chinese Fish 98
Choinka 99
CHV 2.1 136
Cinderella 99
Claws 333
Clipper 100
Clock 343
CMOS Killer 131
CMOS4 67
Coffeeshop 100
Coffeeshop.1568 101
Coffeeshop.Mte 101
Cohen, Fred 22, 34
Colors 339

 Copyright © Dr Solomon's Software

Colors.B 340
Columbus Day 110
Com2Con 101
Companion viruses 9
Computer Ogre 232
Concept 340
Concept virus 7
Concept.B.Fr 341
Contact addresses vi
Cookie 294
Corgi 307
Corrupted programs 5
CPAV 29
CPW 101
CPW.1527 102
Cracker Jack 30
Crazy Boot 102
Crazy Daisy 103
Crazy Eddie 104
Creeping Death 121
Crew 1 104
Crew 2 105
Cruel 105

D
d 149
D2D 295
D3 67
Da'Boys 105
DaBoys 105
Dallas Cowboys 105
Damage 12, 106
- Major 13
- Minor 12
- Moderate 13
- Severe 13
- Trivial 12
- Unlimited 13

Damage-b 106
Damien 287
Daniela 287
Danish Tiny 106
Dark Angel 32, 34
Dark Angel's Multiple Encryptor 34
Dark Avenger 28, 31, 53
Dark Avenger 1800 107
Dark Avenger 2 108
Dark Avenger 2000 108
Dark Avenger 2100 108
Dark Avenger Slowdown 109
Dark Avenger.1530 108
Dark Avenger.1801 108
Dark Avenger.Milena 108
Dark Avenger.MIR 108
Dark Avenger.Ps!ko 108
Dark Lord 109
Dark Ray 34
Dark Slayer 35
Darth 109
Darth Vader-2 110
Darth Vader-3 110
Darth Vader-4 110
Datacrime 110
Datacrime 1b 111
Datacrime 2-2b 111
Datalock 111
Datalock.a-f 111
Date 337
David 111
Dazzler 177
Dbase 112
DBF 112
Dead On Arrival 30
Death March 363
December 24th 166
Deicide 113
Deicide-2 113
DelWin 113
Delwin.1199 114
Delwin.1759 114
Demon 114
Demoralised Youth 30
Den Zuko 1 115
Den Zuko 2 114
Den Zuko 2.a 115
Den Zuko 3 115
DenZuk 114
Desperado.1403 115
Desperado.1403a-c 116

Copyright © Dr Solomon's Software

Destructor 116
Devil's Dance 117
Devil's Dance.941 117
Devil's Dance.b 117
Dewdz 118
DH2 119
Diablo 118
Diablo_boot 118
Diamond 119
Diamond.V1024 119
Diamond-b 119
Diamond-Damage 106
Diamond-David 111
Diamond-Greemlin 151
Diamond-Lucifer 197
Diana 107
Die Hard.3000 120
Die Young 108
Die-Hard 119
Die-Hard.4000a-c 120
Die-Lamer.1098 120
Dinamo Empire.INT.10.b 287
Dir 122
DIR II 121
DIR II.a 122
Dirvir 122
Dis 234
Discom 122
Disk crunching 165
Disk eater 165
Disk Filler 123
Disk Killer 232
Disk Ogre 232
Divina 342
DMV 343
Do nothing 288
Donald 287
Doom II Death 295
Doom II.1240 124
Doom II.752 124
Doom2Death 295
DOS Boot Record 6
DOS boot sector 6
DOS-62 322
DOS-68 322
Doteater 125
Dr. Popp 27
Droppers 6
DSME.Demo 125
DSME.Teacher 125
Durban 268
Dutch-555 258
Dyslexia 125
Dyslexia dropper 126

E
Eccles 83
Eddie 2 108
Eddie 3 108
Eddie 4 108
Eddie-1 107
EDV 126
EICAR 29
Eight Tunes 127
Eight Tunes.1971 127
Ekaterinburg 264
EMF 270
Empire 127
Empire. Monkey 128
Empire.1-2 128
Empire.a-d 128
Empire.B.4 128
Empire.D1-D2 128
Empire.Evil 128
Empire.Monkey 128
Empire.Monkey.a 287
Empire.Monkey.a-b 287
Empire.Monkey.B 129
Empire.U of A 128
Empire.UA 128
Enemy 270
Enigma 129
Enigma.b 129
Epbr 286
erusalem-T1 174
Espejo 129
Essex 257
Esto te pasa 129
Etc 130
European 29

 Copyright © Dr Solomon's Software

Evil 131
Evil Empire 127
Evil Genius 229
Evil One 351
EXE_Bug 131
EXE_Bug.Hooker 132
Exebug 131
Exebug.a-e 132
Explosion-11 234
Exterminator 132

F
F1-337 133
Faggot 134
Falling Letters Boot 134
False alarms 2
Fast infectors 8, 10
Fat Avenger 134
Faust 97
FaxFree 214
Feint 135
Fichv.2_1 136
Fichv.2_1.905 136
Fifth Generation 29
Fifty Boot 263
Filedate 11 136
Filehider 11 136
Filehider 11.V789 136
Filler 123
Filler.a 124
Filler.b 124
Filler-6 123
Find 151
Findme 137
FindVirus 17
Finnish Sprayer 138
Finnish.357 138
Finnish.378 138
Finnish.709a-b 138
First Austrian 322
Fish 139
Fish Boot 98
Fish6 139
Fist 270
Flash 140
Flip 140
Flip.2153.a 141
Flip.2343.a 141
Flip.2343.b 141
Flushed 287
Form 141
Form 18 141
Form May 141
Form.a 142
Form.b 142
Form.e 142
FormatC 345
France 363
Frank 142
Frankenstein 142
Freddy 142
Freddy.1870 143
Freddy.1878 143
Free Love 234
French Boot 179
Frère 172
Friday 13th 172, 329
Friday-13th-440 234
Friday-15th (Skism) 175
Friendly 344
Frodo 143
Frodo.4K 143
Frodo.a 143
Frodo.IDF 143
Frodo-b 144
Frogs 144
Fu Manchu 144
Fu Manchu.2086 144
Fumble 145
Fumble.b-d 146
Fumble.c-d 146
F-You 133

G
Galicia 146
Gdynia.680 253
GENB 146
Generic Decryption Engine 35
Generic decryption engine 53
Genius 229

Copyright © Dr Solomon's Software

GENP 147
Gergana 147
Germs 6
Ghost 148
Ghostballs 148
Ginger 148
Ginger.2691 149
Ginger.2774 149
Ginger.2848 149
Ginger.Orsam.2620 149
Ginger.Orsam.2624 149
Gingerbread 148
Glut 30
Goblin 113
GoldBug 149
GoldBug.a-f 150
Gonorrhoea 30
Good Times 150
GP1 150
Grain of Sand 201
Greemlin 151
Green Caterpillar 151
Green Caterpillar.1575 151
Green Caterpillar.1591 151
GreenStripe 152
Grower-268 153
Grower-268V270X 153
Guess 345
Guppy 154

H
Hacker 160
Hahagif 154
Hallöchen 155
Hammer 65
Happy New Year 1600 221
Harakiri 155
Harare 289
Hare.7610 156
Hari 156
Hate 156
Havoc 220
Hawaii 286
HDEuthanasia 156
Headcrash 157
Hebrew University 172
Hebrew University of Jerusalem 22
Hello 1a 155
Helloween 157
Helloween.1182 158
Helloween.1227 158
Helloween.1288 158
Helloween.1376a-f 157
Helloween.1384 158
Helloween.1401 158
Helloween.1447 158
Helloween.1839 158
Helloween.1888 158
Hellpit 30
Hemp 286
Hero 159
Hidden 143
Hidenowt.1741 159
High Integrity Computing Laboratory 24
HIV-1 169
HLL.ow.12288 162
HLLC.Even_Beeper 159
HLLO.Harakiri 155
HLLO.Messanger 162
HLLO.Novademo 162
HLLO.Novademo.a-c 163
Hoaxes 4
Holland 292
Holland Girl 292
Hong Kong 286, 293
Horse 160
Horse 2 160
Horse 3 160
Horse 4 161
Horse 5 161
Horse 6 161
Horse 7 161
Horse Boot 161
Hot 346
How viruses are spread 14
Hungarian-482 163
Hybryd 163
Hymn 164
Hymn-2144 165

Copyright © Dr Solomon's Software

I
Icelandic 165
Icelandic 1-b 165
Icelandic 2 166
Ides of March Virus Conference 33
IHC 256
Imposter 346
In love 287
Incom 166
India 254
Infector 266
INT 7F 135
Int13 166
Intended viruses 5
Internal 167
Internal.1381 167
Invader 65
IR&MJ 168
Irish 201
Iskey 260
Israeli 172
Istanbul 168
Istanbul.1312 169
Istanbul.1349 169
Italian 243
Italian Virus Research Laboratory 30
IVL 169

J
J&M 176
Jabberwocky 170
Jack Ripper 262
Jack the Ripper 262
Jackal 171
Japanese Christmas 171
Jeff 171
Jerspain 174
Jeru-Clipper 100
Jeru-Discom 122
Jeru-GP1 150
Jeru-Kylie 188
Jerus3 198
Jerusalem 172
Jerusalem.1244 172, 175
Jerusalem.1808 172
Jerusalem.1808.Standard 175
Jerusalem.1813 172
Jerusalem.Mummy.1364. 176
Jerusalem-113b 174
Jerusalem-Apocalypse 174
Jerusalem-b 172
Jerusalem-Captain Trip 175
Jerusalem-Czech 174
Jerusalem-Frère.2 174
Jerusalem-J 175
Jerusalem-Jan25 175
Jerusalem-Nemesis 175
Jerusalem-Sat13 174
Jerusalem-T13 174
Jerusalem-Westwood 174
Jerusalem-Yellow 175
Jimi 176
Jimi.a-b 176
Jimmy 176
Jocker 177
Jojo 177
Joker 177
Joker-01 178
Jokes 4
Joshi 178
Joshua 178
July 13 179
Jumper 179
June 16th 180
June 4 180
June 4th.a 287
June 7 171
JuneTunes 303
Junkie 181
Justice 182
JV 172

K
Kaczor.mp.4444 182
Kamasya 183
Kamikaze 241
Kampana.a 184
Kampana.mp.d 146
Kampana-3445 183
Kampana-boot 297

Copyright © Dr Solomon's Software

Kaos4 184
Kaos4.697 184
Keeper.Lemming 190
Kemerovo 184
Kemerovo.V257 184
Kennedy 106
Keydrop 185
Keypress 185
Keypress.a-e 186
Keytrick 186
Khafir, Masud 33
Khetapunk 64
Kiev 287
Kiev-483 186
Kitty 186
Klaeren 156
KOH-Compress 285
Korea Boot 222
Kranz 293
Krsna 156
Kukac Turbo 187
Kukac-Nagytud 187
Kylie 188

L
Laodung 287
Laroux 356
Lazy 188
LBC 222
LBNYJ 350
Leapfrog 189
Leapfrog.V516 189
Leech 189
Legislation 15
Lehigh 22, 189
Lehigh University 22
Lemming 190
Lemming.2144 191
Lemming.2151 191
Lemming.2160 191
Lenart 66
Lennon 96
Leprosy 191
Leprosy-B-D 192
Leszoptad 192
Liberty 193
Lisa2 286
Lisbon 193
Lisbon.b-d 194
Little Brother 194
Little Brother.276 195
Little Brother.299 195
Little Brother.300 195
Little Brother.301 195
Little Brother.307 195
Little Brother.321 195
Little Brother.349 195
Little Pieces 195
Little Red 195
Little Red Book 195
Live after Death 1 196
Live after Death 2 196
Live after Death 2.V1226 196
Live after Death 3 131
Live after Death 4 241
Live after Death 5 255
LiXi 66
Lovechild 197
Lred 195
Lucifer 197
Luz (Advert 249
Lyceum 209
Lzr 287

M
Mac 198
MAC22 198
MacGyver 198
MacGyver.2803 a-d 199
MacGyver.2824 199
MacGyver.3160 199
MacGyver.4112 199
MacGyver.4480 199
MacGyver.4643 199
MacGyver.4645 199
Macho 293
Macro viruses 7
Macrosoft 293
Magnitogorsk 199
Magnitogorsk-2048 200
Major 200

 Copyright © Dr Solomon's Software

Major.1644 200
Major.1692 200
Maltese Amoeba 201
Mange Tout 201
Mange Tout.1099 201, 202
Manitoba 287
Many Fingers 202
Manzon 203
Manzon.1404 203
Manzon.1414 203
Mao 195
Mardi 204
Marijuana 286
Markt 204
Markt.1533 205
Markt.1548 205
Markt.1551 205
Markt.MG1-MG3 205
Master Boot Record 6
Matteo 263
MCGY 198
McGyv 198
Mediamarkt 204
Mediera 101
Mendoza 175
Merritt 358
Mexican 117, 287
MG 205
MGTU 205
Michelangelo 206
Microbe 206
Micropox 356
Mierda 101
Migram 207
Migram-Cemetery 208
Migram-Smack 208
Milous 227
Minnow 360
Minsk-1075 208
Mirea 209
Mirea.1086 209
Mirea.1766 209
Mirea.1773 209
Mirea.1788 209
Mirea.1800 209
Mirea.1813 209
Mirea.1888a-b 209
Mirea.1901 209
Mirea.1950 209
Mirea.1975 209
Mirea.2087 209
Mirea.2204 209
Mirea.4157 209
Mirea.703 209
Mirea.930 209
Mirea.958 209
Mirror 209
Miscellaneous objects of infection 10
MISiS 210
MISIS.a-d 210
Mistake 243, 244
Mix 1 210
Mix 2 211
Mix1-b 211
Mixer1 210
MLTI 260
Mongol 212
Mongolian 212
Mongolian Boot 212
Monkey 128, 286
Monkey 2, 286
Month 4-6 212
Month 4-6.a-b 213
Monxla 213
Morbus Waiblingen 172
Mosquito 213
Motherfish 334
Mule 214
Multipartite viruses 9
Mummy 2.1 172
Murphy 214, 289
Murphy-1 214
Murphy-1-3 215
Murphy-2 214
Music virus 236
Musicbug 216
Musician 236
Mutation Engine 35, 53

Copyright © Dr Solomon's Software

N
Nado 216
Nado.02 216
Nado.584 216
Nado.759 216
Nado.838 216
Nado.841 216
Nagytud 187
Natas 217
Naughty Hacker 160
Necrophylia-b 219
Necropolis 218
Necros.1164 219
Nemesis 351
Network protection 19
Neuro.Havoc 220
Neurobasher.N8Fall 220
Neuroquila 220
Neuville 179
New York Boot 231
New Zealand 286
Newboot 1 256
NewBug 67
Nightfall 220
Nightfall.4518a-b 221
Nightfall.4527 221
Nightfall.5767 221
NIKA 210
Nina 221
Nina 2 222
Nina. V1600 221
Nina-256 222
NJH 222
NJH2LBC 222
NJH2LBC.a. 223
NJH-LBC 222
No Bock 223
No INT.a 287
No_Frills 223
No_Frills.1358 224
No_Frills.813 224
No_Frills.815ab 224
No_Frills.835 224
No_Frills.840 224
No_Frills.843 224
No_Frills.950 224
No_Frills.Dudley.1153 225
Nocargar 249
Noint 225, 287
Nomen 226
Nomenklatura 226
Nomenklatura.a-b 226
Non-Canadian 128
Nondes 83
Non-TSR file viruses 8
Noon-beep 227
NOP 286, 287
Nop 347
Norton AntiVirus 29
Norton, Peter 24
NotB 230
Nov 17.1006 228
Nov 17.1007 228
Nov 17.584 228
Nov 17.690 228
Nov 17.706a-b 228
Nov 17.768 228
Nov 17.800a-c 228
Nov 17.855a-b 228
Nov 17.864 228
Nov 17.880 228
Nov 17.900a-c 228
Nov 17.998 228
Nov17 227
November_17th 227
Nowhere Man 32
Npox.963 229
Npox.963.a-c 229
Nuclear 347
Nuclear.1332 241
Nuclear.B 348
Nuke.Pox 229
Nulls 287
Number 1 60
Number 1.b 231
Number of the Beast 230
Number of the Beast.666 230
Number of the Beast.V512 230
Number One 231
NYB 231

 Copyright © Dr Solomon's Software

NYB.B1 231

O
Odious.569 232
Ogre 232
Old Yankee 233
Omega 234
Omicron 140
Omicron 2 140
ON 64 234
ON 64.V696 234
One-Half 234
Ontario.1024 236
Oropax 236
Overwriting viruses 9

P
Paris 237
Paris.TCC 237
Parity 237
Parity.b 237
Parity.boot.enc 256
Partition sector 6
Path companion 9
Pathogen 277, 278
Payday 172
PC Business World 27
PC Byte Bandit 303
PcVrsDs 238
Peking 358
Perfume 239
Perfume.blank 240
Perfume.message 240
Perfume.Slash 240
Perfume-731 240
Peter 240
Peter II 240
PH33R.1332 241
Phoenix 1226 196
Phoenix 800 196
Phoenix Evil 131
Phoenix phoenix 241
Phoenix Proud 255
Phx 242
PHX.1015 242
PHX.1289 242
PHX.1295 242
PHX.1360 242
PHX.823 242
PHX.965 242
Pichincha 303
Pile, Christopher 37
Pindonga.3580 243
Ping Pong 243
Ping Pong-B 243
Pinworm 244
Pinworm.1800 245
Pinworm.2150 245
Pinworm.2171 245
Pinworm.2371 245
Pinworm.2400 245
Pinworm.2566 245
Pinworm.2585 245
Pinworm.2780 245
Pirates Hat.2360 245
Piter 246
Pixel 246
Pixel-275 248
Pixel-277 248
Pixel-283 248
Pixel-295 248
Pixel-299 248
Pixel-779 248
Pixel-837 248
Pixel-847 248
Pixel-850 248
Pixel-854 247
Pixel-877 247
Pixel-892 247
Pixel-897 247
Pixel-899 247
Pixel-899b 247
Pixel-905 247
Pixel-Year-6545 248
PKZ300 trojan 249
Plague 250
Plastique 65
Poetcode 83
Polimer 251
Polite 349

Copyright © Dr Solomon's Software

Polymorphism 11
Possessed 251
Possessed.b 252
Prague Blinker 73
Prague Joker 73
Prague Shaker 73
Prank Macro 340
Predator 252
Predator 2 252
Predator.2424 253
Predator.2448 253
Pretentious.680 253
Pretoria 180
Print Screen Boot 254
Print Screen Boot.a 255
Print Screen-1024 254
PrnSn 254
Procedures 15
Proud 255
Prudents 256
Prudents.1210 256
PSQR 174
PUX 242
Pux 242

Q
Qrry 257
Quandary 256
Queeg 278
Queit, Profesor. 265
Query 257
Quit-1992 258
Quit-1992.555 258
Quit-1992.B 258
Quox 258

R
Radai, Yisrael 22
Raubkopie 259
Ray Joke 259
RC-1049 260
RCE-1206 318
RCE-1339 319
Red Cross 63
Red Diavolyata 260
Redx 63
Revenge 260
Reverse.948.a-b 262
Riot Evil 284
Ripper 262
Rostov 287
RPS 263
RPS2 263
Rules 15
Russ-1075 208
Russian 172
Russian Flag 264
Russian Mirror 264
RVPS 311

S
Sadam 265
Sampo 265
Sampo.69 265
Samsoft 186
San Diago 286
Sanded 286, 287
Sarampo 266
Sarampo.1371 267
Sarampo.1450 267
Sarampo.1470 267
Saratoga 165
Sat Bug.Sat Bug 267
Satan 198
Satan Bug 267
Satria 268
Satria.a-c 268
Saturday 14th 268
SAYAWAT 269
Sayha.4000 269
SBC 236
SBlank 142
Scanners 16, 17
Scotts Valley 270
Screamer 270
Screaming Fist II 270
Screaming Fist II.692 271
Screaming Fist II.696 271
Screaming Fist II.724 271
Screaming Fist II.732 271

 Copyright © Dr Solomon's Software

Screaming Fist II.838 271
Screen+ 1 271
Screen+1.V948 271
Sea 210
SEA Zharinov 210
Search 114
Sector Zero 271
Self Mutating Engine 31
Semaj 30
Sentinel 272
Sentinel.1-5 272
Seoul 358
Sex Revolution 286
Sex Revolution 1.1-2 287
Shadowbyte 272
Shake 273
She Has 273
Shoo 198, 274
SI-492 275
Sibylle.858 275
Sigalit 318
SillyBop 179
Simulate 276
Siskin-Hero-506 159
Skism 32
Sleep_Walker 332
Slovak Bomber 234
Slow 361
Slow infector 10
Slowdown 109
SMEG v0.1 277
SMEG v0.2 278
SMEG.Pathogen 277
SMEG.Queeg 278
Smithsonian 286
Soft-236 210
Solano 125
Sonus 287
Spanish 306
Spanish-Telecom-3 146
Spanz 279
Sparse 279
Squeaker 279
St Leos 185
Stack 280
Staf 280
Stakka 129
Standard.a 287
Stardot-600 281
Stardot-789 281
Stardot-789.805 281
Stardot-789.a 282
Starship 282
Stat 284
Staycool.573 284
Stealth 11
Stealth 2 258
Stealth techniques 46
StealthBoot 285
StealthBoot.a-f 286
StealthBoot.KOH.a-c 286
Stoned 128, 286
Stoned dropper 287
Stoned.Angelina 64
Stoned.Satria 268
Stoned-16-a 287
Stoned-8 287
stoned-floppy 287
Stonehenge 286
Striker 287
STSV 288
Stupid 288
sUMsDOS 172
Sunday 172
Sunday 1 Tenseconds 173
Sunday 1.b 173
Sunday 1.d 173
Sunday 2 173
Sunday.a 173
Sunday.b 173
Suomi 288
Superhacker 289
SVC 289
SVC 3.1 290
SVC 5.0 289, 290
SVC 6.0 290
SVC.3103.a 290
Sverdlov 165
SVIR 290
Swami 291

Copyright © Dr Solomon's Software

Swedish Disaster 287
Swiss 292
Swiss Army 292
Swiss Boot 292
Swiss Boot.a-c 292
Swiss-143 291
Swoboda, Franz 21
Sydney 361
Sylvia 292
Sylvia.a-d 293
Symantec 29
Syslock 293
Syslock.3551 293

T
Tai-Pan.434 294
Tai-Pan.438 295
Tai-Pan.438.a-b 295
Tai-Pan.666 295
Taiwan 3 65
Taiwan 4 65
Taiwan Doom II.1240 124
Taiwan Doom II.725 124
Taiwan-708 296
Taiwan-743 296
Talentless Jerk 289
Tannenbaum 354
Tardy, John 34
Tchechen 297
Tchechen.1909 297
Tchechen.1919 297
Tchechen.3430 297
Tchechen.3470 297
Tchechen.3560 297
TEKRAR 307
Telecom 183
Telefonica 297
Tenbytes 298
Tenbytes.1554 298
Tenbytes.1559 298
Tenbytes.9800
0000 298
Tentacle 299
Tequila 299
Tequila.2468.a-c 300
Tequila.2469 300
Teraz.b-e 287
Terror 300
Testvirus B V1.4 300
Thanksgiving 301
Thanksgiving.V1253 301
The Aids Information Diskette 5
The Black Baron 37
The Greek 70
The Rat 302
Thirteen minutes 302
Thirteen minutes.V711 302
Three_Tunes.1784 303
Thursday-12th 303
Tiny 304
Tiny-127 304
Tiny-128 305
Titz 273
Topsy-905 72
Tornado 305
Traceback 306
Traceback.3066 306
Track Swap 307
Tracker 242
Trakia 307
Trakia.1070 308
Trakia.561 308
Trakia.570 308
Trakia.661 308
Trash 308
Traveller 108
Tremor 308
Tremor.4000.a-c 309
Trident 33
Trident Polymorphic Engine 33
Trivial 309
Trkswap 307
Trojans 4
Trojector 310
Trojector.1463 310
Trojector.1561 310
TSR file viruses 8
TSR scanner 17
Tumen 310
Tumen.1092 311

Copyright © Dr Solomon's Software

Tumen.1242 311
Tumen.1255 311
TUQ 311
Turbo 265
Turin 243
Turku 185
Twelve 312
Twelve Tricks 312
Twin 314
Twins 185
Typo 145
Typo Com 145

U
Ugur 307
Unashamed 315
Unesco 322
University of Delaware 21
University of Turin 23
University of Wellington 22
Urkel 315
Uruguay.1-8 317
Uruguay.6 316
Uruguvau 316
Usenet 298
USSR 136
USSR-1049 260
USSR-707 317
USSR-707.V707 317

V
V1028 109
V1721 361
V2000 108
V2100 108
V2480 104
V2P6 317
V905 72
Vacsina 359
Vacsina.TP-05 318
Vacsina.TP-05.a 318
Vacsina.TP-16 319
Vacsina.TP-16.a 319
Valert 298
Van Wyk, Ken 22
vapourware 31
Vbasic 319
Vbasic.B 320
Vbasic.C 320
VCL.Markt 204
VCL-3..DI 204
VCL-Werbe 204
Vcomm 320
Vcomm.637 320
Vcomm.A 320
VCS 330
VDV-853 320
Venezualan 114
Vera Cruz 243
VFSI 321
Victor 321
Vienna 322
Vienna.348 323
Vienna.353 323
Vienna.367 323
Vienna.435 323
Vienna.510 323
Vienna.528 323
Vienna.535 323
Vienna.582 323
Vienna.583 323
Vienna.622 323
Vienna.623 323
Vienna.627 323
Vienna.644 323
Vienna.645 323
Vienna.646 323
Vienna.646b 323
Vienna.648 322, 323
Vienna.656 323
Vienna.716 323
Vienna.733 323
Vienna.822 323
Vienna.W13B 323
Vienna-1881 99
Vienna-534 323
Vienna-648 322
Vienna-71a1 323
Vienna-744 323
Vienna-Iraqui 323

Copyright © Dr Solomon's Software

Vinchuca.925 324
Violator 325
Violator B3 326
Violator B4 327
Violator-Arf 326
Violator-arf.s 326
Virdem 327
Virdem Disktrash 328
Virdem English 328
Virdem.2 328
Virdem-1542 328
Virogen 37
Virogen.Pinworm 244
Virtual device drivers 16
Virus Bulletin 28
Virus Clinic Unit 33
Virus Construction Set 330
Virus Creation Laboratory 32
Virus naming 55
Virus-101 328
Virus-90 329
Virus-B 329
Virus-B.423 329
VirusGuard 17
VLamix 120
Vogel, Fred 26
Voronezh 330
Voronezh-600 331
VP 331
Vriest 332
V-Sign 318
VX BBS 29

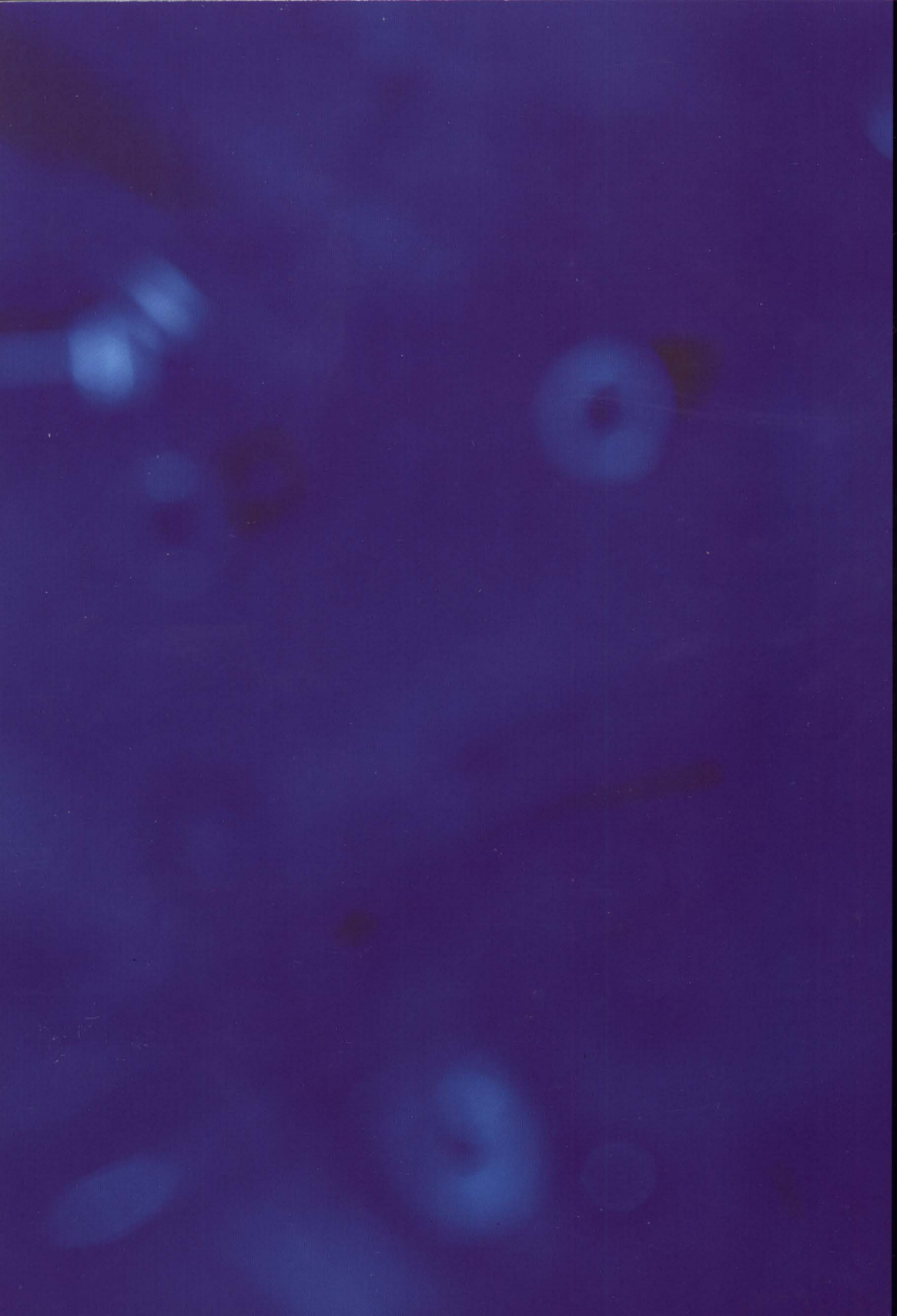
W
W13.A 323
Wabik 177
Walker.3846 332
Warrior 333
Washburn, Mark 23, 28
Watpu 269
Wazzu 350
WBMV 340
W-Boot 286, 287
WD1 287
WD7 287
Wedding 220
Weinacht 354
WelcomB 77
Werewolf 333
Werewolf.1152 334
Werewolf.1168 334
Werewolf.1208 334
Werewolf.1267 334
Werewolf.1361 334
Werewolf.1500 334
Werewolf.1500a-b 334
Werewolf.658 334
Werewolf.678 334
Werewolf.684a-b 334
Werewolf.685 334
WeWo 333
Whale 334
Whit 286
Wiederoffnen 351
WinGuard 18
Winlamer 335
WinWord.Concept 340
WinWord.Nop 347
WinWord.Wazzu 350
Wisconsin 336
Witcode 337
Wllop 265
WM.AntiDMV 337
WM.Atom 338
WM.Colors 339
WM.Colors.B 340
WM.Concept 340
WM.Concept.B.Fr 341
WM.Divina 342
WM.DMV 343
WM.Extra 343
WM.FormatC 345
WM.Friendly 344
WM.Guess 345
WM.Hot 346
WM.Imposter 346
WM.NOP 347
WM.Nuclear 347
WM.Nuclear.a-b 348
WM.Nuclear.B 348

 Copyright © Dr Solomon's Software

WM.Polite 349
WM.Telefonica 350
WM.Wazzu 350
WM.Wazzu.a-f 350
WM.Wiederoffnen 351
WM.Xenios 351
Wolfman 352
Wonderful 328
WordMacro 241
WordMacro.Atom 338
WordMacro.Color 339
Wordmacro.Hot 346
WordMacro.Nop 347
WordMacro.Wazzu 350
WW-217 352
WW217.a 353
WW6Infector 340
WW6Macro 340
WWT-01 353
WWT-02 353
WXYC 353
WXYCa-b 354

X
XA1 354
XBoot 307
Xenios 351
Xeram 355
Xeram.1664 355
XM.Laroux 356
Xmas 294, 355
XPEH 356
XPEH.4016 356
XPEH4 356
XPEH5 356
XTREE 33
Xtree 29

Y
Yale 358
Yale Boot 358
Yankee Doodle 359
Yankee-1202 358
YD.TPXX 359
Youba 83
Yukon 359

Z
Zany.143a 291
Zapper 286, 287
Zaraza 58
Zbug 361
Zero Bug 361
Zero Eater 361
Zero-hunt1 360
Zero-hunt2 360
Zerotime 361
Zero-to-O 361
Zharinov 210
Zherkov 362
Zherkov.1010 363
Zherkov.1023 363
Zherkov.1915 363
Zherkov.1958 363
Zherkov.2960 363
Zherkov.2968 363
Zherkov1882 363
ZK900 363

Copyright © Dr Solomon's Software